PART 2

The Tate Profile

Definition 4. Assume $E[m] \subseteq E(\mathbb{F}_q)$ and let (P_1, P_2) be a basis for $E[m]$. Then, the *m-Tate profile* is the map

$$t_{[m]} : E(\mathbb{F}_q) \to \mu_m^2, \qquad Q \mapsto \left(\, t_2(P_1, Q), \, t_2(P_2, Q) \, \right).$$

For $Q \in E(\mathbb{F}_q)$, we say that $t_{[m]}(Q)$ is the *m-profile* of Q. When $t_{[m]}(Q) = (1,1)$, we say the profile is *trivial*.

1

If the Tate pairing t_m is bilinear, then the Tate profile $t_{[m]}$ is linear.

2

If the Tate pairing t_m is non-degenerate, then $\ker t_{[m]} = [m]E(\mathbb{F}_q)$.

Thus, $t_{[m]}(Q)$ is trivial if and only if there is an $R \in E(\mathbb{F}_q)$ with

$$[m]R = Q.$$

3

Together, $t_{[m]}$ gives us isomorphisms

$$E[m] \; \cong \; E(\mathbb{F}_q)/[m]E(\mathbb{F}_q) \; \cong \; \mu_m^2.$$

Thus, the basis (P_1, P_2) together with $t_{[m]}$ gives us *coordinates*.

Example 1

Theorem 3. For an elliptic curve $E : y^2 = (x - r_1)(x - r_2)(x - r_3)$ with $r_i \in \mathbb{F}_p$, we have $P \in [2]E(\mathbb{F}_p)$ if and only if $(x_P - r_1)$, $(x_P - r_2)$, and $(x_P - r_3)$ are squares.

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

PART 2

The Tate Profile

Definition 4. Assume $E[m] \subseteq E(\mathbb{F}_q)$ and let (P_1, P_2) be a basis for $E[m]$. Then, the *m-Tate profile* is the map

$$t_{[m]} : E(\mathbb{F}_q) \to \mu_m^2, \qquad Q \mapsto \left(t_2(P_1, Q),\ t_2(P_2, Q) \right).$$

For $Q \in E(\mathbb{F}_q)$, we say that $t_{[m]}(Q)$ is the *m-profile* of Q. When $t_{[m]}(Q) = (1,1)$, we say the profile is *trivial*.

1

If the Tate pairing t_m is bilinear, then the Tate profile $t_{[m]}$ is linear.

2

If the Tate pairing t_m is non-degenerate, then $\ker t_{[m]} = [m]E(\mathbb{F}_q)$.
Thus, $t_{[m]}(Q)$ is trivial if and only if there is an $R \in E(\mathbb{F}_q)$ with

$$[m]R = Q.$$

3

Together, $t_{[m]}$ gives us isomorphisms

$$E[m] \;\cong\; E(\mathbb{F}_q)/[m]E(\mathbb{F}_q) \;\cong\; \mu_m^2.$$

Thus, the basis (P_1, P_2) together with $t_{[m]}$ gives us *coordinates*.

Example 1

Theorem 3. For an elliptic curve $E : y^2 = (x - r_1)(x - r_2)(x - r_3)$ with $r_i \in \mathbb{F}_p$, we have $P \in [2]E(\mathbb{F}_p)$ if and only if $(x_P - r_1)$, $(x_P - r_2)$, and $(x_P - r_3)$ are squares.

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

Theorem 3. We have $P \in [2]E(\mathbb{F}_p)$ if and only if $t_{[2]}(P)$ is trivial.