

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

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

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

$$[m]R = Q.$$



La Siesta (1982)

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

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

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*.



La Siesta (1982)