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 4

Theorem 6. Let E be an elliptic curve over $\mathbb{F}_q$ of order $h \cdot r$, with r a large prime, and h a small cofactor. For $P \in E(\mathbb{F}_q)$, we may verify $P \in E[r](\mathbb{F}_q)$ either by

a.) $[r]P = \mathcal{O}_E$, or,

b.) when the h-Tate pairing t_h is non-degenerate by triviality of $t_{[h]}(P)$.

La Siesta (1982)

The agenda for today

PART 1
The Tate Pairing

PART 2
The Tate Profile

PART 3
Generalisations