PART 2

The Tate Profile





La Siesta (1982)

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

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*.





linear. IS

is bilinear, then the Tate profile

If the Tate pairing









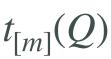
is trivial if and only if there is an

is non-degenerate, then

If the Tate pairing



 $\ker t_{[m]} = [m]E(\mathbb{F}_q)$

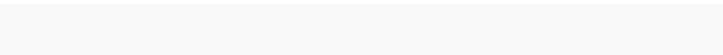


Theorem 3. For an elliptic curve $E: y^2 = (x - r_1)(x - r_2)(x - r_3)$ with $r_i \in \mathbb{F}_p$, we have $P \in [2]E(\mathbb{F}_p)$ if and only if $(x_P - r_1)$, $(x_P - r_2)$, and $(x_P - r_3)$ are squares.

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

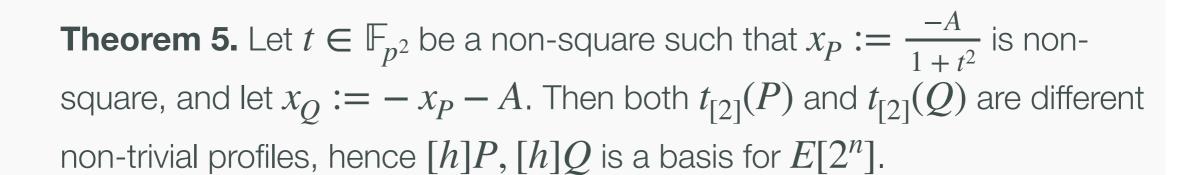


Theorem 4. Let $E: y^2 = x^3 + Ax^2 + x$ be a Montgomery curve over \mathbb{F}_{p^2} with $2^n \mid p+1$ and 2-torsion $L_1=(0,0), L_2=(\alpha,0),$ and $L_3=(\frac{1}{\alpha},0).$ Then, for $P\in E[2^n]$ we have $[2^{n-1}]P=L_i$ if and only if $t_2(L_i,P)=1$ and $t_2(L_i,P)\neq 1$ for $i\neq i$.



Theorem 4. For $P \in E[2^n]$, the profile $t_{[2]}(P)$ determines $[2^{n-1}]P$.

Theorem 5. Let $E: y^2 = x^3 + Ax^2 + x$ be a Montgomery curve over \mathbb{F}_{p^2} with $2^n \mid p+1$, and let $h = \frac{p+1}{2^n}$. Let $t \in \mathbb{F}_{p^2}$ be a non-square such that $x_P := \frac{-A}{1+t^2}$ is also non-square, and let $x_Q := -x_P - A$. Then, the points $P = (x_P, y_P)$ and $Q = (x_Q, y_Q)$ give a basis [h]P, [h]Q for $E[2^n]$.



Together, $t_{\lceil m \rceil}$ 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.

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 4. Let $E: y^2 = x^3 + Ax^2 + x$ be a Montgomery curve over \mathbb{F}_{p^2} with $2^n \mid p+1$ and 2-torsion $L_1=(0,0), L_2=(\alpha,0),$ and $L_3=(\frac{1}{\alpha},0).$ Then, for $P\in E[2^n]$ we have $[2^{n-1}]P=L_i$ if and only if $t_2(L_i,P)=1$ and $t_2(L_i,P)\neq 1$ for $j\neq i.$



Theorem 4. For $P \in E[2^n]$, the profile $t_{[2]}(P)$ determines $[2^{n-1}]P$.