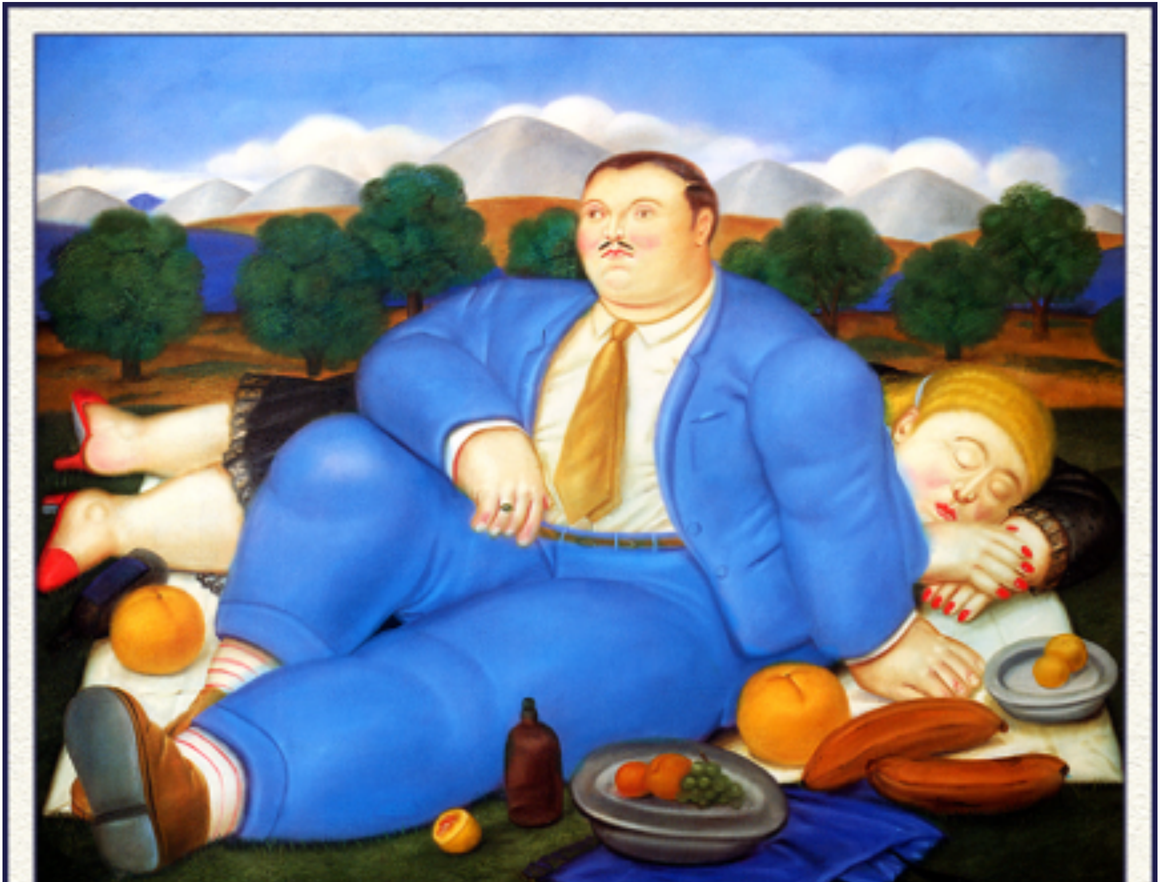
PART 2

The Tate Profile

KU LEUVEN



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

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

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

is linear.

If the Tate pairing

is bilinear, then the Tate profile

t_m

$$t_{[m]}$$

2

If the Tate pairing

is trivial if and only if there is an

Thus,

with

is non-degenerate, then

t_m

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

$$t_{[m]}(Q)$$

$$R \in E(\mathbb{F}_q)$$

$$[m]R = Q$$

Example 3

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 $E[2^n]$.

Theorem 5. Let $t \in \mathbb{F}_{p^2}$ be a non-square such that $x_P := \frac{-A}{1+t^2}$ is non-square, and let $x_Q := -x_P - A$. Then both $t_{[2]}(P)$ and $t_{[2]}(Q)$ are different non-trivial profiles, hence $[h]P, [h]Q$ is a basis for $E[2^n]$.

Example 2

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

$$t_2(L_i, P) = 1 \text{ and } t_2(L_j, P) \neq 1 \text{ for } j \neq i.$$

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

3

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

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

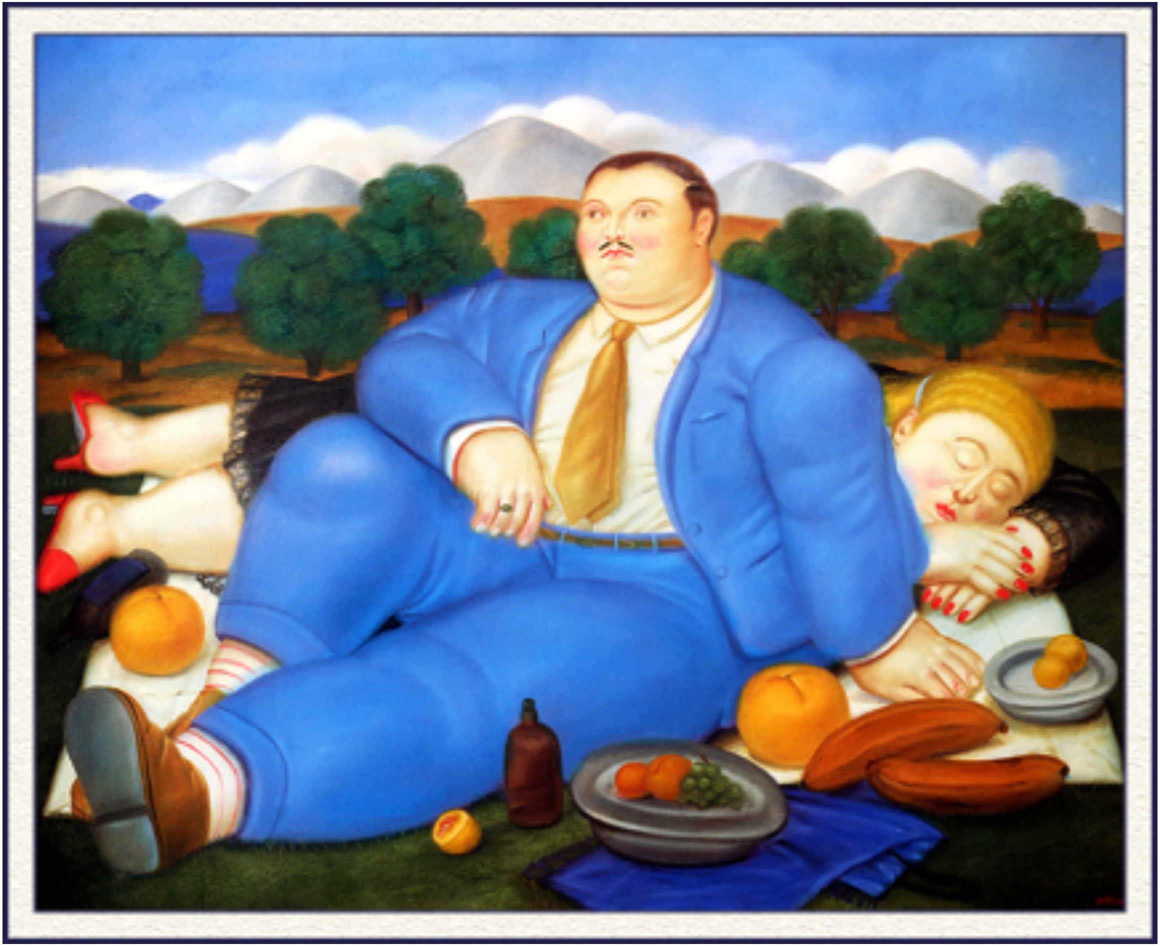
Thus, the basis (P_1, P_2) together with $t_{[m]}$ gives us *coordinates*.

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)

Example 3

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 $E[2^n]$.

Theorem 5. Let $t \in \mathbb{F}_{p^2}$ be a non-square such that $x_P := \frac{-A}{1+t^2}$ is non-square, and let $x_Q := -x_P - A$. Then both $t_{[2]}(P)$ and $t_{[2]}(Q)$ are different non-trivial profiles, hence $[h]P, [h]Q$ is a basis for $E[2^n]$.