PREVIOUSLY...

- Weierstrass models
- Isogenies
- The Tate module

$$T_p(\mu) = \varprojlim \mu_{p^n} \cong \mathbb{Z}_p$$

$$T_p(E) = \varprojlim E[p^n] \cong \mathbb{Z}_p \oplus \mathbb{Z}_p$$

Theorem Let E/K be an elliptic curve, and let $m \geq 2$. There is a pairing

$$e_m : E[m] \times E[m] \longrightarrow \mu_m \qquad \left((S,T) \longmapsto e_m(S,T) = \frac{g_T(X+S)}{g_T(X)} \right)$$

s.t. e_m is:

(a) Bilinear: $e_m(S_1 + S_2, T) = e_m(S_1, T) \cdot e_m(S_2, T)$

$e_m(S, T_1 + T_2) = e_m(S, T_1) \cdot e_m(S, 1$