

PREVIOUSLY...

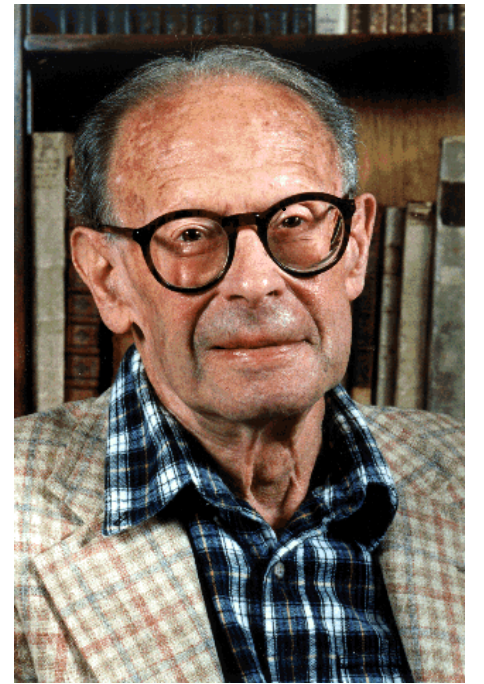
- Isogenies, the dual isogeny
- Inverse limits and the Tate module

$$T_p(\mu) = \varprojlim \mu_{p^n}, \quad T_p(E) = \varprojlim E[p^n]$$
$$\varprojlim \mathbb{Z}/n\mathbb{Z} = \hat{\mathbb{Z}}, \quad T(\mu) = \varprojlim \mu_n, \quad T(E) = \varprojlim E[n]$$

TODAY...

- The Weil pairing

André
Weil
(1906 - 1998)



Recall:

$$\left[\begin{array}{l} \sigma: \text{Pic}^0(E) \xrightarrow{\sim} E \\ [D] \longmapsto P \end{array} \right]$$

s.t. P is the unique pt on E
w/ $D \sim (P) - (O)$.

Corollary

Let E be an elliptic curve, and let $D = \sum_{P \in E} n_P \cdot (P)$ be a divisor of degree 0. Then D is principal iff $\sum_{P \in E} [n_P] \cdot P = O$.

addition on E .

Pf.

$$D \sim O \text{ (principal)} \iff \sigma(D) = O$$

$$\iff \sigma\left(\sum_{P \in E} n_P \cdot (P)\right) = O$$

$$\iff \sigma\left(\sum_{P \in E} n_P \cdot (P) - \left(\sum_{P \in E} n_P\right) \cdot (O)\right) = O$$

$$\begin{array}{l} \deg D = 0 \\ \Downarrow \\ (\sum n_P = 0) \end{array}$$

$$\iff \sigma\left(\sum_{P \in E} n_P \cdot ((P) - (O))\right) = O$$

$$\iff \sum [n_P] \cdot \underbrace{\sigma((P) - (O))}_P = O \iff \sum [n_P] \cdot P = O. \quad \blacksquare$$

Construction of the Weil pairing.

E elliptic curve / K . Let $T \in E[m]$. Consider $m \cdot (T) - m \cdot (\mathcal{O})$.

NOTE: $[m] \cdot T - [m] \cdot \mathcal{O} = \mathcal{O} - \mathcal{O} = \mathcal{O}$, and $\deg(\nearrow) = m - m = 0$.

$\xrightarrow{\text{COR}}$ $\exists f \in \bar{K}(E)$ s.t. $\text{div}(f) = m \cdot (T) - m \cdot (\mathcal{O})$.

Let $T' \in E$ be s.t. $[m]T' = T$. ($[m]$ is a non-ct. isog \Rightarrow surjective)

NOTE: $[m]^*(T) - [m]^*(\mathcal{O})$ (Recall: $\phi^*((\mathcal{Q})) = \sum_{P \in \phi^{-1}(\mathcal{Q})} \mathcal{O}_\phi(P) \cdot (P)$)

$$= \sum_{R \in E[m]} (T' + R) - \sum_{R \in E[m]} (R)$$

$$\searrow \text{deg} = 0 - m^2 - m^2$$

$$\searrow \sum_{R \in E[m]} T' + R - \sum_{R \in E[m]} R = \sum_{R \in E[m]} T' = [m^2]T' = [m]T = \mathcal{O}$$

$\xrightarrow{\text{COR}}$ $\exists g$ s.t.

$$\text{div}(g) = \sum_{R \in E[m]} (T' + R) - \sum_{R \in E[m]} (R)$$

$$f \text{ s.t. } \operatorname{div}(f) = m \cdot (T) - m \cdot (G) \quad \text{w/ } T \in E[m]$$

$$g \text{ s.t. } \operatorname{div}(g) = \sum_{R \in E[m]} (T' + R) - \sum (R)$$

NOTE: $\operatorname{div}(g^m) = m \cdot \operatorname{div}(g) = \sum_{R \in E[m]} m(T' + R) - m \cdot (R)$

$$\operatorname{div}(f([m])) = m \cdot \left(\sum_{R \in E[m]} (T' + R) - (R) \right)$$

$$f([m])(Q) = 0 \Rightarrow f([m]Q) = 0$$

\Rightarrow $f([m])$ and g^m differ by a factor of \overline{K}^*

\Rightarrow Pick f so that $f \circ [m] -$

