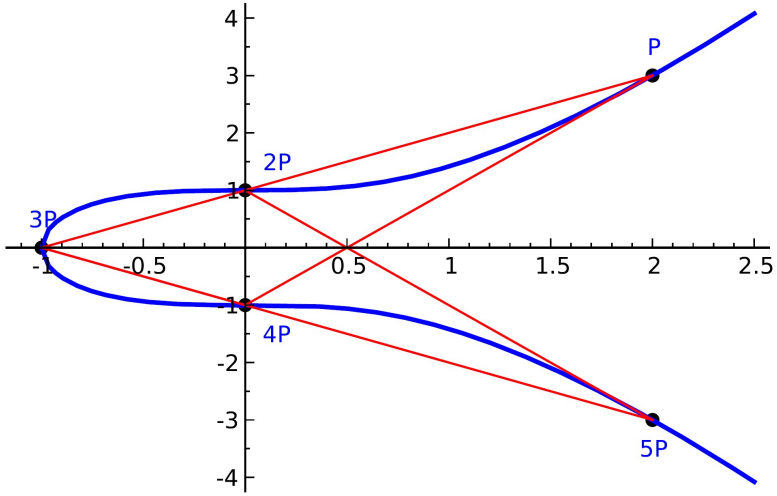
MATH 5020
THE ARITHMETIC OF ELLIPTIC CURVES

INSTRUCTOR: ÁLVARO LOZANO-ROBLEDO

EMAIL: ALVARO.LOZANO-ROBLEDO@UCONN.EDU

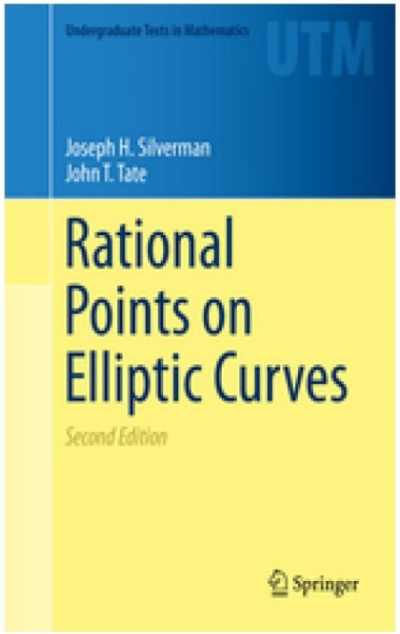
WEB: ALOZANO.CLAS.UCONN.EDU

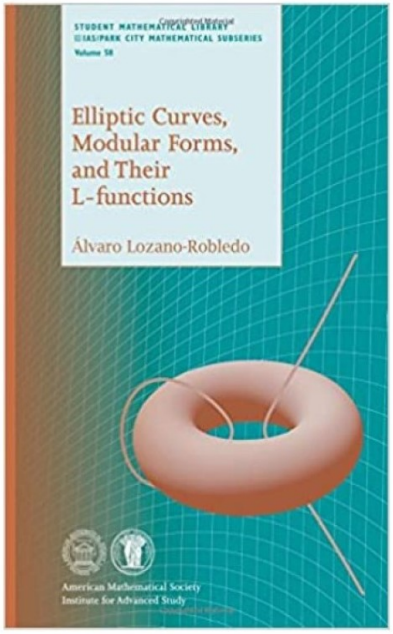
OFFICE HOURS: (check email)



The elliptic curve $E/\mathbb{Q} : y^2 = x^3 + 1$ has a point $P = (2, 3)$ of order 6.

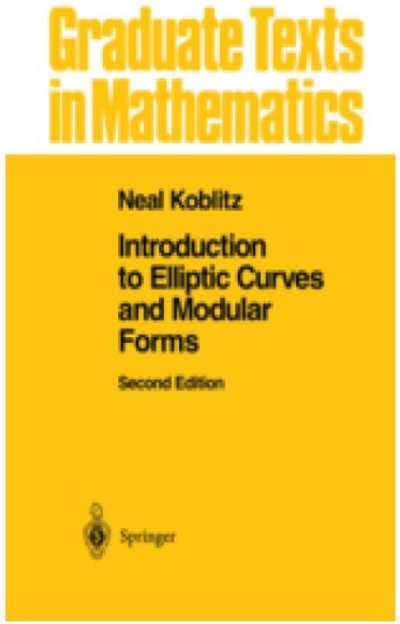
ABOUT BOOKS ...

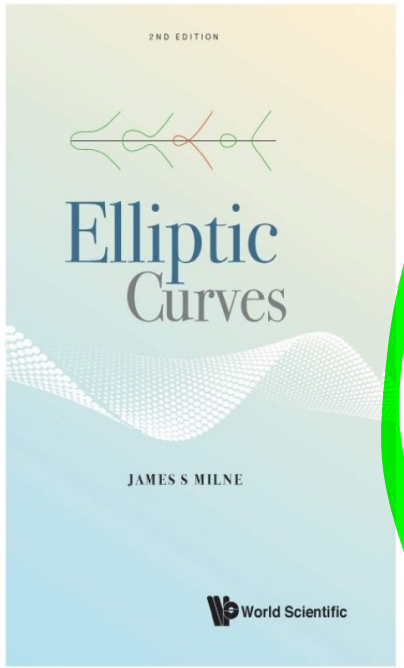


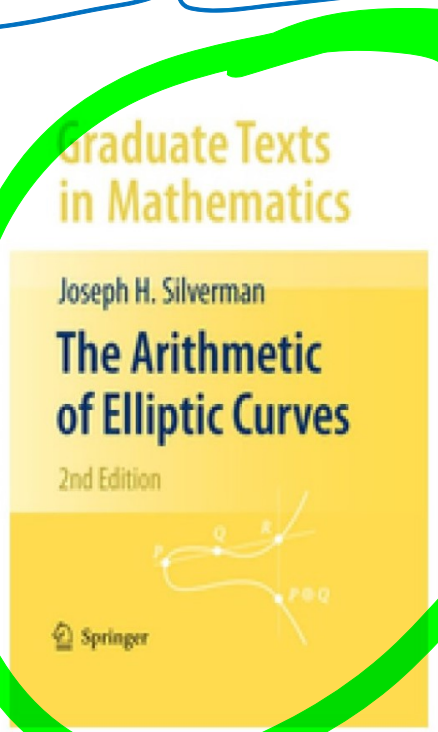


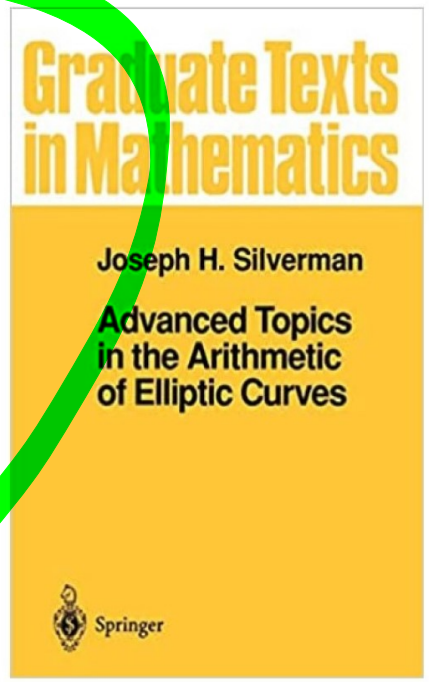
undergrad level

grad level

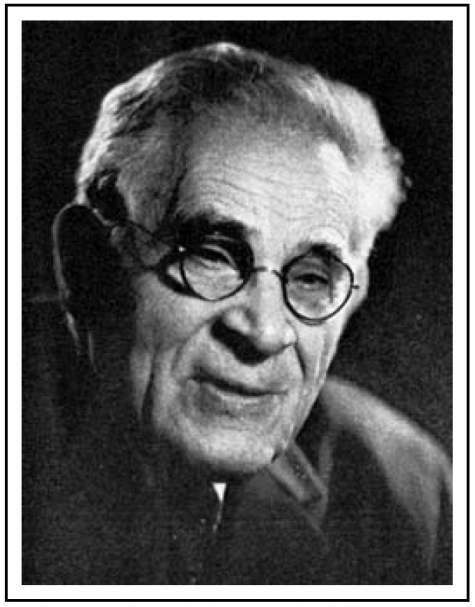








GOAL OF THE COURSE ...



Louis Mordell
1888 – 1972

André Weil
1906 – 1998

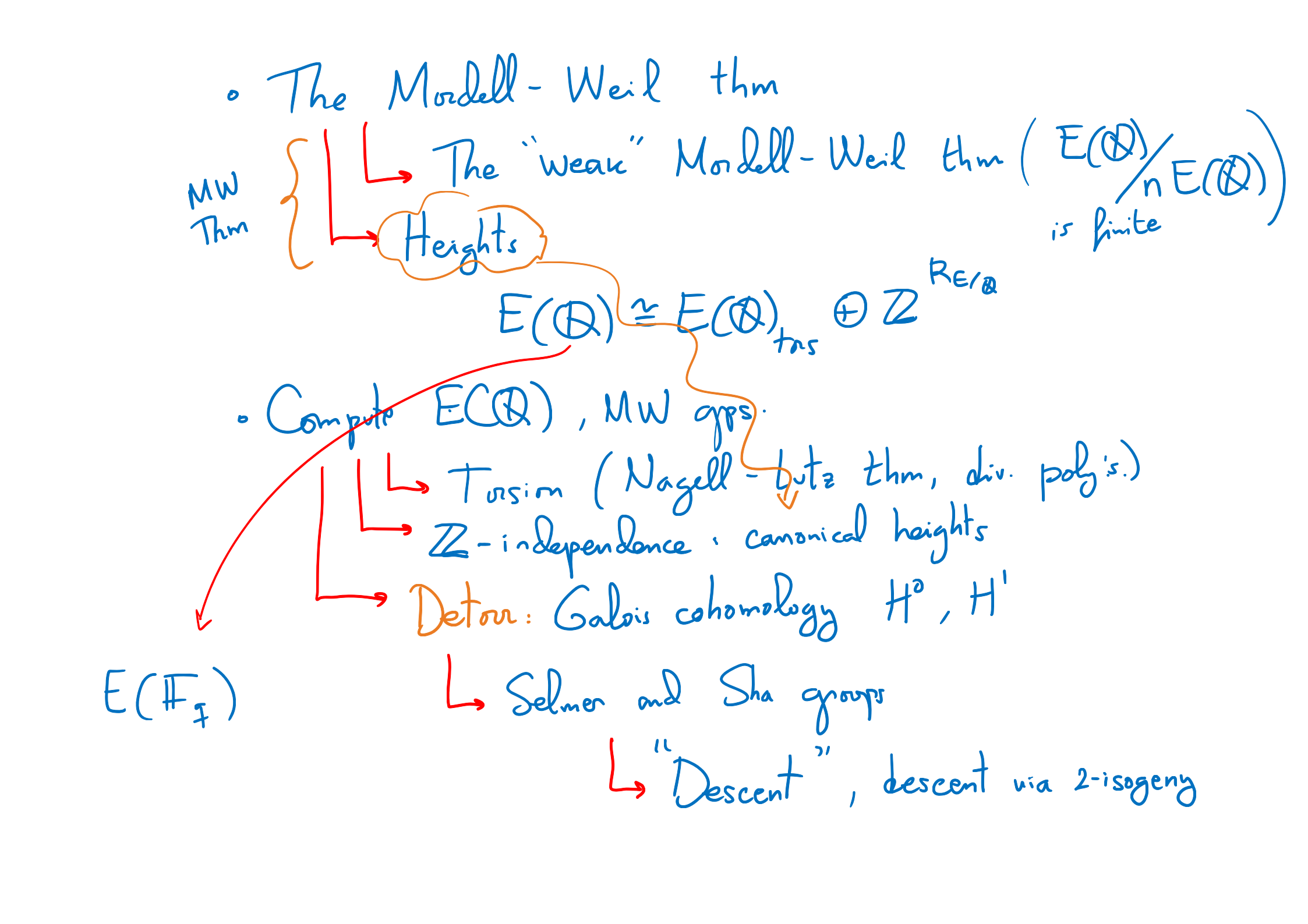
Thm. (Mordell-Weil) Let F be a number field, and let E/F be an ell. curve. Then, $E(F)$ is a finitely generated abelian group. Thus,

$$E(F) \cong E(F)_{tors} \oplus \mathbb{Z}^{R_{E/F}}.$$

Poincaré

Plan.

- Basics of Alg. Geom. (Curves, Varieties, ..., Riemann-Roch)
- Basics of ell. curves
  - Weierstrass models ($y^2 = x^3 + Ax + B$)
  - The group law (twice)
  - Tools: isogenies, Tate module, Weil pairing
- Elliptic curves over $\mathbb{C}$ $\quad E(\mathbb{C}) \cong \mathbb{C}/\Lambda$
- Detour: Formal groups.
- Elliptic curves over fin. fields (Weil conjectures)
  - over local fields ($E/\mathbb{Q}_p$)
  - Points of finite order
  - Good and bad red'n.
  - Ramification in division fields


The Mordell-Weil thm
MW Thm
The "weak" Mordell-Weil thm (E(Q)/nE(Q) is finite
Heights
E(Q) ≅ E(Q)_tors ⊕ Z^Rk_Q
Compute E(Q), MW gps.
Torsion (Nagell-Lutz thm, div. poly's.)
Z-independence: canonical heights
Detour: Galois cohomology H^0, H^1
E(F_p)
Selmer and Sha groups
"Descent", descent via 2-isogeny