

# Arithmetic of Elliptic Curves

S. Lamy and E. Hallouin - [slamy@math.univ-toulouse.fr](mailto:slamy@math.univ-toulouse.fr), [emmanuel.hallouin@univ-tlse2.fr](mailto:emmanuel.hallouin@univ-tlse2.fr)

## Abstract:

The reading seminar will follow the book “The Arithmetic of Elliptic Curves”. We will cover a choice of topics from the following list:

**III.1** Weierstrass Equations

**III.2** The Group Law

**III.3** Elliptic Curves

**III.4** Isogenies

**III.5** The Invariant Differential

**III.6** The Dual Isogeny

**III.7** The Tate Module

**III.8** The Weil Pairing

**III.9** The Endomorphism Ring

**III.10** The Automorphism Group

**V.1** Number of Rational Points

**V.2** The Weil Conjectures

**V.3** The Endomorphism Ring

**V.4** Calculating the Hasse Invariant

## References:

Joseph H. Silverman, *The Arithmetic of Elliptic Curves*, Springer (2nd Edition).