

MATH 595 Elliptic Curves

CRN 42963 / Section EC

2:00 - 2:50 pm, MWF, 141 Altgeld Hall

Meets 28-Aug-17 - 20-Oct-17.

Instructor: Iwan Duursma, AH303

Prerequisite: MATH 530 Algebraic Number Theory

The course covers the basic theory of elliptic curves leading up to a proof of the Mordell-Weil theorem over number fields. We follow chapters 1-8 and 10 in *The Arithmetic of Elliptic Curves*, by J.H. Silverman, Springer GTM 106.

For the minicourse format we will streamline the presentation of the early chapters.

We start with general properties of an elliptic curve over an arbitrary algebraically closed field (non-singular cubic curves, addition law on the rational points, Weierstrass normal form, j -invariant, endomorphism ring, automorphism group). Then we consider properties of elliptic curves over finite fields (number of rational points, Hasse-Weil theorem, supersingular curves), over local fields (singular cubic curves, good and bad reduction, torsion subgroup), and finally over number fields (rational points, torsion points, Mordell-Weil theorem, Selmer groups, Tate-Shafarevich groups).