

Elliptic Curves (M24)

Tom Fisher

Elliptic curves are the first non-trivial curves, and it is a remarkable fact that they have continuously been at the centre stage of mathematical research for centuries. This will be an introductory course on the arithmetic of elliptic curves, concentrating on the study of the group of rational points. The following topics will be covered, and possibly others if time is available.

Weierstrass equations and the group law. Methods for putting an elliptic curve in Weierstrass form. Definition of the group law in terms of the chord and tangent process.

Isogenies. The degree of an isogeny is a quadratic form. The invariant differential and separability. The torsion subgroup over an algebraically closed field.

Elliptic curves over finite fields. Hasse's theorem and zeta functions.

Elliptic curves over local fields. Formal groups and their classification over fields of characteristic 0. Minimal models, reduction mod p , and the formal group of an elliptic curve. Singular Weierstrass equations.

Elliptic curves over number fields. The torsion subgroup. The Lutz-Nagell theorem. The weak Mordell-Weil theorem via Kummer theory. Heights. The Mordell-Weil theorem. Galois cohomology and Selmer groups. Descent by 2-isogeny. Numerical examples.

Pre-requisites

Familiarity with the main ideas in the Part II courses *Galois Theory* and *Number Fields* will be assumed. The first few lectures will include a review of the necessary geometric background, but some previous knowledge of algebraic curves (at the level of the Part II course *Algebraic Geometry* or the first two chapters of [3]) would be very helpful. Later in the course, some basic knowledge of the field of p -adic numbers will be assumed.

Preliminary Reading

1. J.H. Silverman and J. Tate, *Rational Points on Elliptic Curves*, Springer, 1992.

Literature

2. J.W.S. Cassels, *Lectures on Elliptic Curves*, CUP, 1991.
3. J.H. Silverman, *The Arithmetic of Elliptic Curves*, Springer, 1986.

Additional support

Four examples sheets will be provided and four associated examples classes will be given. There will be a revision class in the Easter Term.