Elliptic Curves (L24)

Adam Morgan

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.

Topics likely to be covered include:

- Geometry of elliptic curves: Weierstrass equations, the group law, isogenies.

- Overview of elliptic curves over the complex numbers.

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

- Elliptic curves over local fields: minimal models, reduction modulo p, singular Weierstrass equations, the formal group.

- Elliptic curves over number fields: the torsion subgroup, heights, the Mordell–Weil theorem, Galois cohomology, Selmer groups and descent.

Prerequisites

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 brief review of the necessary geometric background, but this will assume some previous knowledge of algebraic curves, at the level of the Part II course Algebraic Geometry or the first two chapters of [1]. Later in the course, some basic knowledge of the Part III course Local Fields will be assumed.

Literature

1. J.H. Silverman, *The Arithmetic of Elliptic Curves*, Springer, 1986.

2. J.W.S. Cassels, *Lectures on Elliptic Curves*, CUP, 1991.

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

Additional support

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