3705 (Elliptic Curves)

Year:	2014–2015
Code:	MATH3705
Level:	Advanced
Value:	Half unit (= 7.5 ECTS credits)
Term:	2
Structure:	3 hour lectures per week
Assessment:	100% examination
Normal Pre-requisites:	MATH7202
Lecturer:	Dr RM Hill

Course Description and Objectives

This is a course in number theory. An elliptic curve is an equation of the form $y^2 = x^3 + ax^2 + bx + c$, where a, b, c are given rational numbers. The aim of the course is to be able to find the solutions (x, y) to this equation with x and y rational numbers. The methods used are from geometry and algebra.
The study of elliptic curves is an important part of current research in number theory and cryptography. It was central to the proof of Fermat's last theorem. There are still many unsolved problems in this area, in particular the Birch–Swinnerton-Dyer conjecture, for which there is a $1 million prize offered by the Clay Institute.

Recommended Texts

J H Silverman and J Tate, *Rational points on Elliptic Curves*, Springer Undergraduate Texts in Mathematics (1992).

Detailed Syllabus

Chapter 1
Introductory material on 2-dimensional projective geometry. The Group law on a cubic. Weierstrass normal form of a cubic. Singularities and Elliptic curves.

Chapter 2
Elliptic functions. Parametrization of the complex points of an elliptic curve using Weierstrass' elliptic functions. Correspondence between the group laws on the curve and on the complex torus.

Chapter 3
Points of finite order. The Nagell-Lutz Theorem;. Calculating the points of finite order on a curve.

Chapter 4
Heights of points on an elliptic curve. Mordell's Theorem. Calculating the rank of some curves.