School of Mathematics

Course 428 — Elliptic Curves, Cryptography & Fermat's Last Theorem 1999-2000
(Optional JS & SS Mathematics, SS Two-subject Moderatorship)

Lecturer: Dr. T.G. Murphy

Requirements/prerequisites:

Duration: 21 weeks

Number of lectures per week: 3

Assessment:

End-of-year Examination: Probably examined in 3 parts, one examination covering each term's work

Description: Two recent events have elevated the theory of elliptic curves from a somewhat specialized topic to the centre of mathematical development.

Firstly, Andrew Wiles' proof of Fermat's Last Theorem in 1995 was set in the context of elliptic curves over the rationals $\mathbb{Q}$.

Secondly, elliptic curve cryptography — based on elliptic curves over finite fields $\mathbb{F}_q$ — is rapidly becoming the standard encryption algorithm.

Elliptic curves are the next most simple curves after straight lines and conics. They are particularly interesting because each elliptic curve carries a natural structure as an abelian group; geometrically, if A, B, C are 3 collinear points on the curve then $A + B + C = 0$. This group structure is the basis for virtually all applications of elliptic curves.

The theory of elliptic curves grew out of Weierstrass' study of doubly-periodic complex functions. (The term 'elliptic' arose from the rôle of such functions in computing the arc-length around an ellipse.)

Today the theory has become an exciting amalgam of complex function theory, algebraic geometry and arithmetic (or number theory).

October 1, 1999