School of Mathematics

Course 428 — Elliptic Curves, Cryptography & Fermat's Last Theorem 2001–02
(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:

Description:

After a century of relative quiescence, during the last 20 years elliptic curves have become one of the hottest areas of mathematical research.

There are two main reasons for this.

Firstly, Andrew Wiles proof of Fermat's Last Theorem in 1997 was set entirely in the context of elliptic curves. Recall that this theorem states that if $n \geq 3$ and $x, y, z \in \mathbb{Z}$ then

$$x^n + y^n = z^n \Rightarrow xyz = 0.$$

The result was proved by showing that if

$$a^n + b^n = c^n$$

were a counter-example to the theorem then the elliptic curve

$$y^2 = x(x - a^n)(y + b^n)$$

would have very strange properties. (In technical terms the curve would not be *modular*.) Wiles showed that every curve of this form *was* modular. It remains an open question whether all elliptic curves over $\mathbb{Q}$ without exception are modular.

The second area of activity is in cryptography. Elliptic curve encryption has become the most-favoured technique for encrypting data, although most e-commerce still uses the older, obsolete, RSA encryption. (Standard RSA encryption as used in most e-commerce can probably be cracked using a fast PC in a few hours.)

Closely related to this is the use of elliptic curves in factoring large numbers (ie containing several hundred digits). This arises in connection with RSA encryption, which is based on the belief that it is very difficult to factor a number of the form $n = pq$ where p and q are large (say, 100-digit) primes.

All these applications are based on the fact that *every elliptic curve has a natural structure as an abelian group*; any two points P, Q on the curve can be added, by a simple construction, to give a third point $P + Q$.

This course will be given in three parts.

The first (and longest) will be devoted to elliptic curves over the rationals $\mathbb{Q}$, leading to Mordell's Theorem that the abelian group in this case is finitely-generated.

The second part will be devoted to elliptic curve encryption, and the third to fctorisation using elliptic curves.

The three parts may be examined separately, at the end of each term; or there may be a single exam. (The decision will probably be left to the class.)

October 4, 2001