MA426 — Term 2

Elliptic Curves — 18 CATS

Status: List C .

Commitment: 30 lectures, plus a willingness to work hard at the homework.

Prerequisites: This is a sophisticated module making use of a wide palette of tools in pure mathematics. In addition to a general grasp of first and second year algebra and analysis modules, the module involves results from MA246 Number Theory (especially factorisation, modular arithmetic), and makes substantial use of the whole of MA3B8 Complex Analysis. Knowledge of some parts of MA3D5 Galois Theory, MA3A6 Algebraic Number Theory, MA4A4 Algebraic Curves or MA4A5 Algebraic Geometry is helpful but not essential.

Orientation: Elliptic curves have a long and glorious history. Their study in number theory goes back to Diophantus in the 3rd century. Examples of elliptic curves are

$$X^4 + Y^4 = Z^2$$

and (the simultaneous pair)

$$X^2 + Y^2 = Z^2, \qquad X^2 - Y^2 = W^2.$$

The problem is to find all rational solutions to these equations. The first was solved by Fermat and the second by Fibonacci (you might want to try them yourself).

Elliptic curves are interesting geometrically because they are the first instances of equations whose solution set cannot be parametrised by rational functions. From the analytic point of view, elliptic curves are parametrized by doubly-periodic functions whose study goes back to illustrious mathematicians as Gauss, Abel, Jacobi and Ramanujan. The analytic theory gives such amazing formulae as

$$\frac{1}{1+\frac{e^{-2\pi}}{1+\frac{e^{-4\pi}}{1+\cdots}}} = \left(\sqrt{\frac{5+\sqrt{5}}{2}} - \frac{\sqrt{5}+1}{2}\right) e^{2\pi/5}.$$

Elliptic curves link number theory, algebraic geometry and complex analysis, and have applications to factorization of integers (a very hard problem for large integers), cryptography and coding theory. Elliptic curves were moreover prominent in Andrew Wiles' famous proof of Fermat's Last Theorem, and are at the forefront of research in number theory and related subjects.

Content: We hope to cover the following topics (in varying levels of detail) and more:

1. Non-singular cubics and the group law; Weierstrass equations.
2. Elliptic curves over complex numbers, elliptic functions.
3. Elliptic curves over the rationals; descent, bounding $E(\mathbb{Q})/2E(\mathbb{Q})$.
4. Resultants, Heights, Mordell-Weil theorem.
5. Elliptic curves over finite fields; Hasse estimate.
6. p-adic fields (basic definitions and properties).
7. 1-dimensional formal groups (basic definitions and properties).
8. Elliptic curves over p-adic fields and reduction mod p.
9. Computation of torsion groups over $\mathbb{Q}$; the Nagell-Lutz theorem.
10. Elliptic diophantine problems.
11. Public keys in cryptography; Pollard's $p-1$ method and the elliptic curve method of factorisation.
12. The Hasse principle, the conjectures of Birch and Swinnerton-Dyer.
13. Proof sketch of Fermat's Last Theorem.

Leads to: Ph.D. studies in number theory or algebraic geometry.

Books:

J. W. S. Cassels, *Lectures on Elliptic Curves*, LMS Student Texts 24, Cambridge University Press, 1991.
A very useful textbook, emphasizing the explicit aspects of the subject. It is however a little old-fashioned with the notation and obscure in places.

J. H. Silverman and J. Tate, *Rational Points on Elliptic Curves*, Undergraduate Texts in Mathematics, Springer, 1992.
A very pleasant introduction, though covers only part of the topics we are interested in.

J. H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics 106, Springer, 1986.
This is an extremely polished and detailed textbook, and every prospective number theorist should read it, but it is a little advanced for our course.
H. McKean and V. Moll, *Elliptic Curves: Function Theory, Geometry, Arithmetic*, Cambridge University Press, 1997.
Emphasis on complex function theory of elliptic curves, which we will not spend much time on.
F. Diamond and J. Shurman, *A First Course on Modular Forms*, Graduate Texts in Mathematics 228, Springer-Verlag, 2005. Covers the relationship between elliptic curves and modular forms which we will only touch on.

Assessment: 15% by a number of assessed worksheets, 85% by 3-hour examination.

Lecturer: Samir Siksek