Course content for MT3120/MT4120, Computational Number Theory

Prerequisites:
MT3110

Aims:
To provide an introduction to many major methods currently used for testing/proving primality and for the factorisation of composite integers. The course will develop the mathematical theory that underlies these methods, as well as describing the methods themselves.

Learning outcomes:
- Be familiar with a variety of methods used for testing/proving primality, and for the factorisation of composite integers.
- Have an introductory knowledge of the theory of binary quadratic forms, elliptic curves, and quadratic number fields, sufficient to understand the principles behind state-of-the art factorisation methods.
- Be equipped with the tools to analyse the complexity of some fundamental number-theoretic algorithms.
- MT4120: demonstrate a breadth of understanding appropriate for an M-level course

Course content:
Background: Complexity analysis; revision of Euclid's algorithm, and continued fractions; the Prime Number Theorem; smooth numbers; elliptic curves over a finite prime field; square roots modulo a prime; quadratic number fields; binary quadratic forms; fast polynomial evaluation.
Primality tests: Fermat test; Carmichael numbers; Euler test; Euler-Jacobi test; Miller-Rabin test; Lucas test; AKS test.
Primality proofs: succinct certificates; p – 1 methods; elliptic curve method; AKS method.
Factorisation: Trial division; Fermat's method, and extensions; methods using binary quadratic forms; Pollard's p – 1 method; elliptic curve method; Pollard's rho and lambda methods; factor-base methods; quadratic sieve; number field sieve.