Course content for MT5412, Computational Number Theory

Prerequisites:
A UG course in number theory

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:
1. Be familiar with a variety of methods used for testing/proving primality, and for the factorisation of composite integers.
2. 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.
3. Be equipped with the tools to analyse the complexity of some fundamental number-theoretic algorithms.
4. Demonstrate independent learning skills

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 roo methods; factor-base methods; quadratic sieve; number field sieve.