# COURSE SPECIFICATION FORM

for new course proposals and course amendments

<table>
<thead>
<tr>
<th>DEPARTMENT OF MATHEMATICS</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Course Code:</strong></td>
<td>MT4120</td>
</tr>
<tr>
<td><strong>Course Value:</strong></td>
<td>0.5</td>
</tr>
<tr>
<td><strong>Status:</strong></td>
<td>Optional</td>
</tr>
<tr>
<td><strong>Course Title:</strong></td>
<td>Computational Number Theory</td>
</tr>
<tr>
<td><strong>Availability:</strong></td>
<td>Term 1</td>
</tr>
<tr>
<td><strong>Prerequisites:</strong></td>
<td>MT3110</td>
</tr>
<tr>
<td><strong>Recommended:</strong></td>
<td>none</td>
</tr>
</tbody>
</table>

## 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:
On completion of the course, students should:
- 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.

## 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.

## Teaching & Learning Methods:
33 hours of lectures and examples classes. 117 hours of private study, including work on problem sheets and examination preparation. This may include discussions with the course leader if the student wishes.

## Key Bibliography:
- A course in number theory and cryptography – N Koblitz (Springer 1994). 512.91 KOB

## Formative Assessment & Feedback:
Formative assignments in the form of 8 problem sheets. The students will receive feedback as written comments on their attempts.

## Summative Assessment:
- **Exam (%)**
  Four questions out of five in a two-hour paper: 100%
- **Coursework (%)**
  None
- **Deadlines:** n/a

The information contained in this course outline is correct at the time of publication, but may be subject to change as part of the Department’s policy of continuous improvement and development. Every effort will be made to notify you of any such changes.