

COURSE SPECIFICATION FORM
for new course proposals and course amendments

Department/School:	Mathematics	Academic Session:	2017-18
Course Title:	Computational Number Theory	Course Value: (UG courses = unit value, PG courses = notional learning hours)	0.5 unit
Course Code:	MT3120	Course JACS Code: (Please contact Data Management for advice)	G100
Availability: (Please state which teaching terms)	Term 2	Status: (i.e.: Core, Core PR, Compulsory, Optional)	Optional Condonable
Pre-requisites:	MT3110	Co-requisites:	-
Co-ordinator:	-		
Course Staff:	-		
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:	<p>1. Be familiar with a variety of methods used for testing/proving primality, and for the factorisation of composite integers.</p> <p>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.</p> <p>3. Be equipped with the tools to analyse the complexity of some fundamental number-theoretic algorithms.</p>		
Course Content:	<p>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.</p> <p>Primality tests: Fermat test; Carmichael numbers; Euler test; Euler-Jacobi test; Miller-Rabin test; Lucas test; AKS test.</p> <p>Primality proofs: succinct certificates; $p - 1$ methods; elliptic curve method; AKS method.</p> <p>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.</p>		
Teaching & Learning Methods:	<p>The total number of notional learning hours associated with this course are 150 hours. 3 lectures per week over 11 weeks. Total 33 hours.</p> <p>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.</p>		
Key Bibliography:	<p>Prime Numbers: a Computational Perspective – R. Crandall and C. Pomerance (Springer 2005). 512.91 CRA</p> <p>A course in number theory and cryptography – N Koblitz (Springer 1994). 512.91 KOB</p> <p>A course in number theory – H.E. Rose (Oxford, 1994)</p>		
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:	<p>Exam: 100% Written Exam. A two hour paper.</p> <p>Coursework: n/a</p> <p>Deadlines: n/a</p>		

Updated September 2017

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.