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:	MT4120	**Course JACS Code:** (Please contact Data Management for advice)	G100
Availability: (Please state which teaching terms)	Term 2	**Status:**	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:	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 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 roo methods; factor-base methods; quadratic sieve; number field sieve.		
Teaching & Learning Methods:	The total number of notional learning hours associated with this course are 150. 3 hours of lectures a week over 11 weeks. 33 hours total. 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:	Prime Numbers: a Computational Perspective – R. Crandall and C. Pomerance (Springer 2005). 512.91 CRA A course in number theory and cryptography – N Koblitz (Springer 1994). 512.91 KOB A course in number theory – H.E. Rose (Oxford, 1994)		
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:** 100% Written exam. A two hour paper. **Coursework:** None		

Updated September 2017