MAS3008 NUMBER THEORY, 2002/3

Lectures:

Monday 10, B93;
Wednesdday 12, C95 (from 16th October);
Thursday 10, B73.

There will be no lectures in Week 7 (18–22 November)

Lecturer: Dr. Nigel Byott (Room 817 - Office Hours: Monday 3, Tuesday 11, Friday 2). Th 12, F 2).

Course web page: http://www.maths.ex.ac.uk/ NPByott/teaching/NT.html, also accessible from the SMS Teaching page. Handouts, example sheets etc will be placed here (mostly as .dvi files).

Assessment: This will be by examination in the summer (75%) and coursework (25%).

The examination will be in the standard form for Level 3 modules (3 hours; Section A (40%) compulsory + Section B (60

The coursework component will consist of indicated questions on each of Examples Sheets 2–5 (equally weighted). Hand-in dates will be on the following Fridays:

Sheet 1 (not assessed)	25 October	(Week 3)
Sheet 2	15 November	(Week 6)
Sheet 3	6 December	(Week 9)
Sheet 4	17 January	(Week 11)
Sheet 5	7 February	(Week 14)

Coursework should be handed in via the box on Level 8 of the Laver Building. Coursework received after the hand-in date will get a maximum of 40%, and coursework more than 2 weeks late will get 0, unless a dispensation has been given by the appropriate Programme Coordinator.

(Almost) all of the lecture material required for each sheet will have been covered at least 2 weeks before the hand-in date.

Recommended Books:
See Student Handbook. Particularly recommended are:
K.H. Rosen *Elementary Number Theory and its Applications,* 3nd edition (Addison-Wesley, 1993).
I. Niven, H.S. Zuckerman & H.L. Montgomery *An Introduction to the Theory of Numbers*, 5th edition (Wiley, 1991).

Course content:

1. **Divisibility and Prime Numbers:** gcd, Euclidean algorithm, primes, unique factorisation.

2. **Congruences:** $\mathbb{Z}_n$, $\varphi(n)$, Fermat's Little Theorem, Euler's and Wilson's Theorems. $x^2 \equiv -1 \pmod{p}$. Solution of linear congruences. Chinese Remainder Theorem. Congruences mod p^n.

3. **Computational Techniques:** Powering algorithm. Pseudo-primes. Miller-Rabin primality test and strong pseudo-primes. Pollard's $p-1$ and Rho factorization algorithms. RSA cryptosystem.

4. **Primitive roots:** Order of an element. Existence of primitive roots mod p^r. Discrete logarithms. Applications to congruences.

5. **Quadratic residues and quadratic reciprocity:** Euler's criterion, Gauss's Lemma, quadratic reciprocity.

6. **Some Diophantine equations:** Sums of 2 and 4 squares, Pythagorean Triples, Fermat's Last Theorem (for $n = 4$).

NPB October 2002