

MAS3008: Number Theory

Lectures: 10am Tuesdays LT6, 11am Thursdays LT6, 2pm Fridays B93, for 11 weeks, starting Tuesday 1 February 2005.

Lecturer: Robin Chapman, room 811, rjc@maths.ex.ac.uk,
web page:

<http://www.maths.ex.ac.uk/~rjc/rjc.html> ,

course web page:

<http://www.maths.ex.ac.uk/~rjc/courses/nt04/nt04.html> .

Brief syllabus:

- **Divisibility and primes:** Prime numbers, factorization, greatest common divisors, Euclidean algorithm.
- **Congruences:** Congruences modulo n , systems of residues, Fermat's theorem, Wilson's theorem, Euler's function, Euler's theorem, linear congruences, Chinese remainder theorem, lifting solutions modulo prime powers, primitive roots.
- **Computational methods:** Fast powering, Fermat test, Miller-Rabin test, Pollard's $p - 1$ and rho methods, RSA cryptography.
- **Quadratic residues:** Quadratic residues and nonresidues, Legendre symbols, Euler's criterion, quadratic reciprocity.
- **Diophantine equations:** Sums of squares, Pythagorean triples, Fermat's last theorem ($n = 4$ case only!).

Recommended Books:

A huge number of introductory texts on number theory have been published. This is just a small selection, from old classics to modern texts.

- R.P. Burn, *A Pathway Into Number Theory* (2nd edition), CUP, 1996.
- H. Davenport, *The Higher Arithmetic* (7th edition), CUP, 1999.
- G.H. Hardy, E.M. Wright, *An Introduction to the Theory of Numbers* (5th edition), OUP, 1979.
- I. Niven, H.S. Zuckerman, H.L. Montgomery, *An Introduction to the Theory of Numbers* (5th edition), Wiley, 1991.
- H.E. Rose, *A Course in Number Theory* (2nd edition), OUP, 1995.
- Kenneth H. Rosen, *Elementary Number Theory and Its Applications* (4th edition), Addison-Wesley, 2000.

Coursework (25%): Five problem sheets will be set fortnightly: only the first four will count towards assessment (equally weighted).

Examination (75%): 2 hours, May/June 2005.