Course content for MT3110, Number Theory

Prerequisites:
MT1810

Aims:
To acquaint students with some of the elementary tools used to analyse the additive and multiplicative structures of the set of integers.

Learning outcomes:
On completion of this course students should be able to:

- handle congruences, including the use of the Chinese Remainder theorem, and the Fermat-Euler theorem;
- manipulate arithmetic functions such as $\tau(n)$, $\mu(n)$, $\phi(n)$ and $o(n)$; and derive some of their basic properties;
- prove the existence of primitive roots modulo a prime and use them in solving certain congruences;
- test for quadratic residues, and use them to answer questions on primes in arithmetic progressions, and representing numbers as sums of two squares;
- find the continued fraction expansion of real numbers, in particular quadratic irrationals, and apply continued fractions to the solution of Pell's equation.

Course content:
Introduction. Revision of material seen in previous years. Integers, primes, factorisation,
congruences including Chinese remainder theorem and the Fermat-Euler theorem.
Arithmetic functions. Introduction to the functions $\tau(n)$, $\mu(n)$, $\phi(n)$ and $o(n)$; product and summation form, Möbius inversion.
Primitive roots. The order of an integer modulo p, primitive roots modulo p, the proof of their existence, the index of an integer modulo p.
Quadratic residues. Legendre's symbol. Euler's criterion for a quadratic residue. Gauss's
Lemma. The law of quadratic reciprocity. Applications to quadratic congruences and primes in arithmetic progressions.
Continued fractions. Definition. Diophantine approximation. Quadratic irrationals and Pell's equation.
Arithmetic functions II. The function $r(n)$ – representing numbers as sums of two squares.