7701 (Number Theory)

Year:	2014–2015
Code:	MATH7701
Level:	Intermediate
Value:	Half unit (= 7.5 ECTS credits)
Term:	2
Structure:	3 hour lectures per week
Assessment:	90% examination, 10% coursework
Normal Pre-requisites:	MATH1202, (MATH2201 recommended),
Lecturer:	Dr RM Hill

Course Description and Objectives
This course is an introduction to elementary number theory. The main focus is on solving equations and congruences in integers, although various other rings will appear in the proofs of theorems.

Recommended Texts
No book does exactly what is in the course, but the following books might be useful:

(i) D. M. Burton, *"Elementary Number Thery"*;

(ii) H. E. Rose, *"A course in number theory"*;

(iii) K. Ireland and M. Rosen, *"A classical introduction to modern number theory"*;

(iv) H. Davenport, *"The higher arithmetic"* (this is mainly for the earlier parts of the course);

(v) J.–P. Serre, *"A course in arithmetic"* (this is a bit more advanced than is needed for the course).

Detailed Syllabus

The Euler totient function φ. We'll show how to calculate $\varphi(n)$. Using this, we'll be able to calculate powers of integers modulo n, and solve congruences of the form $x^a \equiv b \bmod n$.

Existence of primitive roots. In this section we'll prove that for any prime number p, the multiplicative group $\mathbb{F}_p^\times$ is cyclic.

Quadratic reciprocity. Given an integer a, we'll answer the question: for which primes p is a a square modulo p?

Hensel's Lemma. Suppose f is a polynomial, and we have a solution to $f(x) \equiv 0 \bmod p$. We'll show how we can modify the solution to get a solution to $f(x) \equiv 0 \bmod p^n$.

Power series modulo powers of primes. We'll introduce the idea of a power series modulo p^n. In particular introduce the logarithm and exponential functions on $\mathbb{Z}/p^n$ and prove their properties.

The Gaussian integers. The Gaussian integers are numbers of the form $x + iy$ where x and y are integers. We'll prove a theorem describing the the prime Gaussian integers. Using this, answer the question which integers can be written as a sum of two squares.

Continued fractions. We'll describe the continued fraction expansion of a real number. We'll show that this expansion is periodic for real numbers of the form $\sqrt{d}$, and as a consequence we'll find a method for solving Pell's equation $x^2 - dy^2 = 1$.