On-line course materials

MATH32071 - Introduction to Number Theory

Year: 3 - **Semester:** 1 - **Credit Rating:** 10

Aims

This lecture course aims to introduce students to some elementary concepts in number theory. We shall apply some basic algebraic concepts in order to study integer solutions of certain polynomial equations with integer coefficients, such as x^2 + y^2 = z^ (the solutions of which are the so-called `Pythagorean triples).

Whilst there are no official prerequisites for this course, please note that:

- Students who already have some familiarity with groups and other basic algebraic structures may find the material slightly easier than those students who dont.
- A certain level of mathematical maturity is required and you will be expected to work hard!

Brief Description

Number theory is arguably one of the oldest and most fascinating branches of mathematics. This fascination stems from the fact that there are a great many theorems concerning the integers, which are extremely simple to state, but turn out to be rather hard to prove. Even more tantalisingly, there are many simple questions that one can ask about the integers, to which no answer is yet known. It may come as no surprise to you that many of these theorems and open problems relate to the mysterious nature of prime numbers.

In this course we will use a few elementary ideas along with one or two algebraic concepts to prove some appealing statements such as every positive integer is the sum of four squares and there are infinitely many primes of the form 4n+1. We will conclude the course by mentioning a few interesting open problems.

Learning Outcomes

On successful completion of this course unit students will

- Have a sound understanding of divisibility, prime factorisation, modular arithmetic, cyclic groups and primitive roots
- Be able to describe and use the Euclidean algorithm and the RSA algorithm
- Have knowledge and understanding of the Gaussian integers
- Be able to state all of the theorems discussed during the course and apply them to basic problems
- Be able to prove several congruence theorems
- Have an appreciation of some of the unsolved problems in number theory

Syllabus

- Division, primes and the Euclidean algorithm (a review of basic concepts)
- Simple continued fractions (approximation to irrationals; periodicity and quadratic irrationals)
- Diophantine equations (Pell's Equations; Pythagorean triples)
- Congruences (Arithmetic modulo m; linear congruences; Chinese remainder theorem)
- The group of units (Euler's totient function; congruence theorems of Euler, Fermat and Wilson; RSA public key cryptography)
- Primitive roots (Lagrange's polynomial congruence theorem; cyclic groups of units and their generators)
- Quadratic Residues (Legendre symbols; quadratic reciprocity)
- Sums of squares (sums of two squares; sums of four squares; Gaussian integers)

Teaching & Learning Process (Hours Allocated To)

Lectures	Tutorials/ Example Classes	Practical Work/ Laboratory	Private Study	Total
22	11	0	67	100

Assessment and Feedback

Coursework: in-class test weighting 10%

End of semester examination: two hours, weighting 90%

Further Reading

Recommended texts:

- Elements of number theory, Stillwell
- Elementary number theory, Jones and Jones

Staff Involved

Dr Dr marianne johnson Johnson - Lecturer

Data source is EPS system

Back To Top