Course ID 025069

Introduction to Number Theory

MATH 32071

Credit rating 10
ECTS credits 5

Unit coordinator: Marianne Johnson

Semester 1

School of Mathematics
Undergraduate

Level 3

FHEQ level ' Last part of a Bachelors'

Marketing course unit overview
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.

Course unit overview
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.

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 - dy^2 = 1 (Pell's equation).
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 don't.
- A certain level of mathematical maturity is required and you will be expected to work hard!

Learning outcomes

On successful completion of this course unit students will

- Be able to describe and use the Euclidean algorithm and to explain how to solve linear Diophantine equations.
- Be able to describe and use the continued fraction algorithm to (a) find representations of rationals and quadratic irrationals, (b) obtain rational approximations to real numbers and (c) find solutions to Pell's equations.
- Be able to describe the group of units modulo n for fixed value of n, giving information on its group structure and in particular determining the existence of a primitive root modulo n.
- Be able to state and prove several theorems involving polynomial congruences.
- Be able to describe and use the theorem of quadratic reciprocity (and other results) to work with Legendre symbols.

Syllabus

Division, primes and the Euclidean algorithm [2 lectures]

- Introduction to the course and discussion of puzzles and problems involving Diophantine equations.

- A review of basic notions (divisibility, primes, greatest common divisor).

Finite continued fractions [3 lectures]

- Finite simple continued fractions and the continued fraction algorithm.

- Connection to the Euclidean algorithm.

Infinite simple continued fractions [4 lectures]

- Definitions and convergence properties.

- Representation of real numbers; finite/periodic/purely periodic continued fractions.

- Rational approximations of real numbers.

Pell's equations [3 lectures]

- Definitions and examples; trivial solutions and generating positive solutions.

- Using continued fractions to find solutions.

The group of units modulo n [2 lectures]

- A review of basic concepts (modular arithmetic, groups, units) with examples.

- Wilson's theorem, Euler's theorem and Fermat's little theorem

- An application of Euler's theorem (RSA)
Polynomial congruences and primitive roots [3 lectures]

- Applications to Diophantine equations.

- Primitive roots and the structure of the group of units modulo n.
Quadratic residues [3 lectures]

- The group of quadratic residues modulo n.

- Legendre symbols and Quadratic reciprocity.
Sums of squares [2 lectures]

- Fermat's 'two squares' theorem.

- Lagrange's 'four squares' theorem.

Assessment methods

Other	10%
Written exam	90%

Coursework: in-class test weighting 10%End of semester examination: two hours, weighting 90%

Feedback methods
Tutorials will provide an opportunity for students' work to be discussed and provide feedback on their understanding.

Requisites
Students are not permitted to take more than one of MATH32071 or MATH42071 for credit in the same or different undergraduate year.

Available as free choice? N

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

Scheduled activity hours

Lectures	22
Tutorials	11

Independent study hours 67 hours