UNSW SYDNEY

UNSW SCIENCE

SCHOOL OF MATHS AND STATISTICS

MATH3521

Algebraic Techniques in Number Theory

Term 1, 2019

Cricos Provider Code: 00098G

MATH3521 – Course Outline

Information about the course

Course Authority. Dr Chi Mak

Lecturers. Dr Chi Mak RC-4073 chi.mak@unsw.edu.au
Prof Igor Shparlinski RC-5112 igor.shparlinski@unsw.edu.au

Consultation. The time for office hours will be announced during the lectures.

Credit, Prerequisites, Exclusions.

This course counts for 6 Units of Credit (6UOC).

Before attempting this course you must already have gained 12 units of credit in level 2 Mathematics courses. Apart from this, there are no formal prerequisites for MATH3521; however, you will be significantly disadvantaged if you have not already learned certain topics from other courses.

1. You will need to understand properties of the integers such as divisibility, primes, greatest common divisors and congruences, and to be able to perform accurate calculations connected with these topics. If you have studied MATH1081 Discrete Mathematics or MATH2400 Finite Mathematics you should know about these. A set of self-study slides and exercises on assumed knowledge for MATH3521 are available on UNSW Moodle. Maple TA quizzes are available for testing your understanding on the assumed knowledge. **It is essential that you are able to complete the exercises and pass the Maple TA quizzes.** To give yourself the best chance of succeeding in MATH3521 you should do so as suggested in the set of slides.

2. You will need to be familiar with the concepts of vector space, basis and dimension, which you may have learned in MATH1231 or MATH2501.

Exclusions: MATH3711.

Lectures. There will be four hours lecture per week in Weeks 1 to 4 and 6 to 9, two hours per week in Week 5 and Week 10.

Tutorials. There will be one tutorial per week in Weeks 1–10.

Note: Arrangements for the missing lectures due to public holiday will be announced on Moodle.

UNSW Moodle. Further information, lecture/tutorial times and venue, lecture notes and other material will be provided via Moodle.

Course aims

This course examines key questions in the theory of numbers whose solution led to the development of modern abstract algebra. The basic notions of *rings*, *fields*, *groups* and *field extensions* will be developed and used to solve problems relating to the integers, as well as certain geometric problems that interested the ancient Greeks.

Relation to other mathematics courses. Mathematics may be divided into the broad categories of analysis (calculus), algebra, geometry, combinatorics, and logic. This subject fits into the algebra category and follows on from material that you will have learned in first year algebra, linear algebra, and from certain other related courses you may have taken. The course is very useful for those majoring in Pure Mathematics, those planning to teach, and those students of Mathematics who are interested in Number Theory.

Course Learning Outcomes

Students taking this course will develop an appreciation of the basic problems of number theory and the interplay between number-theoretic problems and abstract algebra. The ability to provide logical and coherent proofs of number-theoretic results, and the ability to solve number-theoretic problems via abstract algebraic methods will be paramount.

Through regularly attending lectures and applying themselves in tutorial exercises, students will develop competency in mathematical presentation, and in written and verbal skills.

Relation to graduate attributes. The above outcomes are related to the development of the Science Faculty Graduate Attributes, in particular

- Research, inquiry and analytical thinking abilities;
- Communication; and
- Information literacy.

Teaching strategies underpinning the course

New ideas and skills are introduced and demonstrated in lectures, then students develop these skills by applying them to specific tasks in tutorials and assessments.

Rationale for learning and teaching strategies. We believe that effective learning is best supported by a climate of enquiry, in which students are actively

engaged in the learning process. To ensure effective learning, students should participate in class by attending all classes and preparing effectively for classes (for lectures, by reading through previous lecture notes; for tutorials, by having made a serious attempt to do the tutorial problems before the tutorial). Lectures should be viewed by the student as an opportunity to learn, rather than just copy down lecture notes. Effective learning is achieved when students have a genuine interest in the subject and make a serious effort to master the basic material.

The art of logically setting out mathematics is best learned by watching an expert and paying particular attention to detail. This skill is best learned by regularly attending classes.

Detailed course schedule

It is intended that the following topics will be covered in the given order.
Any variation from this will be indicated by the lecturer.

Chapter 0 – PRESUMED KNOWLEDGE.
(3 hours self-study online materials including online quizzes)

The properties of integers, divisibility, primes and greatest common divisors (gcd), finding gcd of two integers by the Euclidean algorithm and writing the gcd as an integer linear combination of the two number (the Bezout identity), solving simple Diophantine equations and linear Diophantine equations.

Chapter 1 – ABSTRACT ALGEBRA AND THE INTEGERS.
(5 hours lecture, 2 hours tutorial)

The integers, rings and integral domains, divisibility, primes and greatest common divisors, the Euclidean algorithm and the Bezout identity, unique factorisation, principal ideals.

Chapter 2 – DIOPHANTINE EQUATIONS AND CONGRUENCES.
(3 hours lecture, 1 hour tutorial)

Diophantine equations, linear Diophantine equations, congruences, the arithmetic functions d and σ, perfect numbers, Mersenne primes.

Chapter 3 – INTRODUCTION TO GROUPS.
(4 hours lecture, 1 hour tutorial)

Fields, units, groups, isomorphism. The groups $\mathbb{Z}_m$ and $\mathbb{U}_m$; permutation groups and symmetry groups. Wilson's Theorem.

Chapter 4 – THE STRUCTURE OF $\mathbb{U}_m$ AND $\mathbb{Z}_m$.
(5 hours lecture, 1 hour tutorail)

Subgroups, the theorems of Lagrange, Fermat and Euler, cyclic groups, direct products, Chinese Remainder Theorem, primitive roots, exponential congruences.

Chapter 5 – QUADRATIC RECIPROCITY.
(4 hours lecture, 2 hours tutorial)

Quadratic residues, Euler's Criterion, Legendre symbol, Gauss' Lemma, the Law of Quadratic Reciprocity and its applications.

Chapter 6 – THE GAUSSIAN INTEGERS.
(4 hours lecture, 1 hour tutorial)

Norms, units, primes, division, greatest common divisors, ideals and principal ideals in $\mathbb{Z}[i]$, unique factorisation, determination of gaussian primes and the sum of two squares, sums of three and four squares, Waring's Problem.

Chapter 7 – ALGEBRAIC NUMBER FIELDS.
(5 hours lecture, 1 hour tutorial)

Polynomials over fields, degree, division, the Remainder Theorem, roots, prime and irreducible polynomials, Eisenstein's Criterion, algebraic extension field, algebraic number, minimal polynomial, the dimension theorem, complex algebraic extension fields.

Chapter 8 – CONSTRUCTIBILITY.
(4 hours lecture, 1 hour tutorial)

The field of constructible numbers, the classical problems of squaring the circle, trisecting the angle, and duplicating the cube, regular polygons and Fermat primes.

Weekly schedule

Week		Topics	Test
1	Lecture	Abstract Algebra and the Integers	
	Tutorial	Abstract Algebra and the Integers	
2	Lecture	Abstract Algebra and the Integers	
		Diophantine Equations and Congruences	
	Tutorial	Abstract Algebra and the Integers	
3	Lecture	Introduction to Groups	Online quizzes
	Tutorial	Diophantine Equations and Congruences	due 4 pm Friday
4	Lecture	Structure of $\mathbb{U}_m$ and $\mathbb{Z}_m$	Class Test 1
	Tutorial	Introduction to Groups	
5	Lecture	Structure of $\mathbb{U}_m$ and $\mathbb{Z}_m$	
	Tutorial	Structure of $\mathbb{U}_m$ and $\mathbb{Z}_m$	
6	Lecture	Quadratic Reciprocity	
	Tutorial	Quadratic Reciprocity	
7	Lecture	The Gaussian Integers	
	Tutorial	Quadratic Reciprocity	
8	Lecture	The Algebraic Number Fields	
	Tutorial	The Gaussian Integers	
9	Lecture	The Algebraic Number Fields	Class Test 2
		Constructibility	
	Tutorial	The Algebraic Number Fields	
10	Lecture	Constructibility	
	Tutorial	Constructibility	

Assessment

Assessment criteria. The main criterion for marking all written assessment tasks will be clear and logical presentation of correct solutions.

The grading criterion for online web-base assessments will be correct answers correctly entered in the required syntax.

Tests

Rationale. Tests will give students feedback on their progress and mastery of the

material.

Task	Weighting	Duration	Material tested
Online Quizzes	5 %	—	chapter 0
Class Test 1	20%	50 mins	chapters 1 to chapter 4 upto the Chinese Reminder Theroem
Class Test 2	20%	50 mins	chapters 5 to chapter 7

There are two online tests which counts 5 % in total. Details will be provided on Moodle prior to the start of the term. The tests due 4 pm Friday Week 3. Since the test is available in the beginning of the term, deadline will not be extended under normal circumerstances.

The two class test will be held in Week 4 and Week 9 during the last hour of lectures in the weeks. You may bring your own calculator with an affixed "UNSW APPROVED" sticker to the class tests.

If you are absent from a class test because of illness or other circumstances beyond your control, you must apply for Special Consideration on-line within 3 days of the test.

Examination

Duration. Two hours.

Rationale. The final examination will assess student mastery of the material covered in the lectures.

Weighting. 55 % of your final mark.

Calculators. Only calculators with an affixed "UNSW APPROVED" sticker may be used.

For full instructions, see
`www.maths.unsw.edu.au/currentstudents/exam-information-and-timetables`

Additional resources and support

Tutorial Exercises. A set of tutorial exercises will be given out. These problems are for **you** to do to enhance your mastery of the course. Some of the problems may be done by the tutor in tutorials, but you will learn a lot more if you try to do them yourself beforehand.

Lecture notes and/or skeleton notes will appear on Moodle.

Textbooks. There is no set text for this course. The course content will be defined by the lectures and the lecture notes. Any book on number theory may prove useful.

Moodle. All course materials will be available on Moodle. You should check regularly for new materials.

Course Evaluation and Development

The School of Mathematics and Statistics evaluates each course each time it is run. We carefully consider the student responses and their implications for course development. It is common practice to discuss informally with students how the course and their mastery of it are progressing.

Administrative matters

School of Mathematics and Statistics Policies. Students must read and understand the School of Mathematics and Statistics Assessment Policies, found here:

`www.maths.unsw.edu.au/currentstudents/assessment-policies`

Plagiarism and academic honesty. Plagiarism is the presentation of another's thoughts or work as one's own. Issues that you must be aware of regarding plagiarism and the university's policies on academic honesty and plagiarism can be found here:

`my.unsw.edu.au/student/atoz/Plagiarism.html`