SCHOOL of MATHEMATICS and STATISTICS
MATH 3062 NUMBER THEORY AND ALGEBRA
UNIT INFORMATION SHEET, 2012

Lectures
Lectures: Monday 11am, Tuesday 11am and Thursday 1pm in Carslaw 275.

Lecturer: Terry Gagen, Carslaw room 822, phone 02 9351 3194, email terry.gagen@maths.usyd.edu.au

Tutorials
Tuesday at 2pm in Carslaw 453 or Wednesday at 12pm in New Law Annexe 342, according to your printed timetable. Tutorials start in week 2. Rolls are kept in tutorials and students are reminded that satisfactory attendance is a condition of enrolment.

Lecture Notes
I will put a summary of the lectures each week on the MATH 3062 web page.

Consultation
I will be in my office (Carslaw 822) each Monday from 1pm to 2pm for individual help. If you can’t see me at that time, please see me after the lecture and we can make a time suitable to both of us.

Calculators
You will need a calculator in this unit of study. Please note that the university does not provide calculators for use in examinations. Students will be able to use their own calculator in examinations provided it is on the approved list, which is that issued by the NSW Board of Studies for HSC use. Please see

http://sydney.edu.au/current_students/student_administration/examinations/students.shtml#calculators

for the List of Approved Scientific Calculators. You will need to have your personal calculator validated for exam use at the Student Centre.
Web Page

www.maths.usyd.edu.au/u/UG/SM/MATH3062

The web page will contain course material for MATH 3062, including a summary of the lectures, tutorials and solutions, and information about quizzes and assignments.

Reference Books


Assessment

Quiz 1 (12.5%) on Number Theory to be conducted in week 4 (beginning 26 March).
We agreed democratically on 13 March that the first quiz will be in the lecture in Room 275 on Thursday 29 March at 1.00pm. It will contain 10 questions and will be 40 minutes long. All working must be done on the quiz paper. Calculators will be supplied (no personal calculators may be used). I will put a Sample Quiz with solutions on the web next Friday 23 March.

Assignment (5%): to be collected in week 8 (beginning 1 May).

Quiz 2 (12.5%) on Algebra to be conducted in week 12 (beginning 29 May).

Exam (70%): There will be a two-hour examination in June on a date to be announced. More information about quizzes, the assignment and the exam will be made available on the web page closer to the events.
Objectives of this unit of study

The overall objectives of this unit of study are

- to deepen your understanding of arithmetic in $\mathbb{Z}$, and to a lesser extent in $\mathbb{R}$ and $\mathbb{C}$,
- to investigate other algebraic structures which operate under rules which are similar to those which hold in $\mathbb{Z}$,
- to give you insight into how familiar processes in $\mathbb{Z}$ (such as factorisation as a product of primes) can be generalised in more abstract structures,
- to improve your ability to think logically, analytically and abstractly, and to develop your problem-solving skills. (These attributes belong to the ‘Research and Enquiry’ category of the University’s desired generic skills for its graduates.)

The objectives will be achieved through the study of the following specific topics.

**Number Theory:** Modular arithmetic, the Euclidean algorithm, solutions of linear Diophantine equations, continued fractions and their use in approximations, the Gaussian integers, the Fermat-Euler Theorem, the Law of Quadratic Reciprocity, sums of squares, Fermat’s Method of Descent, straight edge and compass constructions and other topics.

**Algebra:** rings, fields, integral domains, polynomial rings, direct sums of rings and the Chinese Remainder Theorem, irreducible elements, unique factorisation, polynomial rings, algebraic numbers.

**Learning Outcomes for Number Theory**

Students who successfully complete the material in the Number Theory half of this unit should be able to

- perform calculations in $\mathbb{Z}$ and $\mathbb{Z}_n$, including finding generators (if they exist) of $\mathbb{Z}_n^*$,
- construct simple proofs of propositions relating to $\mathbb{Z}$ and $\mathbb{Z}_n$,
- solve certain Diophantine equations,
- understand arithmetic in the Gaussian integers $\mathbb{Z}[i]$,
- understand continued fractions and use them to find rational approximations to irrational numbers,
- understand and apply Fermat’s Method of Descent to write an integer as a sum of two squares,
- understand and apply the Law of Quadratic Reciprocity.
Learning Outcomes for Algebra

Students who successfully complete the material in the Algebra half of this unit should be able to

- understand the axioms which define a ring/field/integral domain and be able to identify examples of these structures,
- construct simple proofs of propositions relating to rings, fields, and integral domains,
- find irreducible elements in various integral domains and polynomial rings,
- understand the Chinese Remainder Theorem,
- construct finite fields and other rings of small sizes as quotient algebras of polynomial rings
- understand the existence of generators in finite fields and also the identification of those integers $n$ for which $\mathbb{Z}_n$ has a generator.

Terry Gagen