Lecturer:
Peter Brown (Red Centre 3073; phone: 9385 7055)
email: peter@unsw.edu.au

Units of Credit
This course counts for 3 Units of Credit (3UOC).

Timetable:
Lectures will be held in CLB-2 on Friday 10-12am.
Tutorials There will be one tutorial per week.

Assessment:
Class test 1 (week 5) 10%
Class test 2 (week 11) 10%
Final examination 80%

Class tests:
These will be held in tutorials in Weeks 5 and 11. The tests will last 25 minutes. They will include all the material covered in lectures up to and including the week before the tests. Non-programmable scientific calculators should be taken to the test.

Course Resources
• A detailed set of formal notes will be made available on Blackboard.
• Skeleton lecture notes will be available on Blackboard. These will be the notes used in class.
• A set of exercises (with numerical answers) will be given out in the first lecture.
• Recommended Reading:
• Web-site
  General Information, Problem sets, are available through Blackboard.

Aims:
Since the introduction of digital computers, the importance of discrete and thus finite problems in mathematics has become apparent. For this reason this course, which introduces students to some basic ideas on Finite Mathematics, should prove useful to future Computer Scientists while at the same time providing Mathematics students with an introduction to ideas in Number Theory, the theory of finite fields, cryptography and Algebraic Coding Theory. There is a follow-on course, MATH3411, Information, Codes and Ciphers, which develops the ideas in greater depth.

Objectives:
By the end of this course you should be able to do the following
• Prove theorems and solve problems in basic number theory and algebra in the areas mentioned in the syllabus.

• Apply the above theory to aspects of cryptography and error correcting codes.

**Attendance:**
You are required to attend lectures and tutorials. Rolls will be taken. If you choose not to attend classes, then you may miss out on important information and you will certainly not get the most out of the course.

**Learning and Teaching Philosophy:**
We believe that effective learning is achieved when students attend all classes, have prepared effectively for classes by reading through previous lecture notes, in the case of lectures, and, in the case of tutorials, by having made a serious attempt at doing for themselves the tutorial problems prior to the tutorials.

Furthermore, lectures should be viewed by the student as an opportunity to learn, rather than just copy down lecture notes. The skeleton lecture note approach will greatly facilitate this.

Effective learning is achieved when students have a genuine interest in the subject and make a serious effort to master the basic material.

**Assessment Rationale:**
The class tests will provide feedback on the student’s progress and an opportunity for the student to demonstrate a mastery of the basic techniques and ideas covered up to that point.

**Graduate Attributes:**
Research, inquiry and computational skills, capability and motivation for intellectual development, information technology literacy.

**Teaching Strategies:**
Formal instruction, interactive tutorial exercises, web-based skeleton lecture notes.
Plagiarism

Plagiarism is the presentation of the thoughts or work of another as one’s own.\(^1\) Examples include:

- direct duplication of the thoughts or work of another, including by copying material, ideas or concepts from a book, article, report or other written document (whether published or unpublished), composition, artwork, design, drawing, circuitry, computer program or software, web site, Internet, other electronic resource, or another person’s assignment without appropriate acknowledgement;

- paraphrasing another person’s work with very minor changes keeping the meaning, form and/or progression of ideas of the original;

- piecing together sections of the work of others into a new whole;

- presenting an assessment item as independent work when it has been produced in whole or part in collusion with other people, for example, another student or a tutor; and

- claiming credit for a proportion a work contributed to a group assessment item that is greater than that actually contributed.\(^2\)

For the purposes of this policy, submitting an assessment item that has already been submitted for academic credit elsewhere may be considered plagiarism. Knowingly permitting your work to be copied by another student may also be considered to be plagiarism.

Note that an assessment item produced in oral, not written, form, or involving live presentation, may similarly contain plagiarised material.

The inclusion of the thoughts or work of another with attribution appropriate to the academic discipline does not amount to plagiarism.

The Learning Centre website is main repository for resources for staff and students on plagiarism and academic honesty. These resources can be located via:

www.lc.unsw.edu.au/plagiarism

The Learning Centre also provides substantial educational written materials, workshops, and tutorials to aid students, for example, in:

- correct referencing practices;

- paraphrasing, summarising, essay writing, and time management;

- appropriate use of, and attribution for, a range of materials including text, images, formulae and concepts.

Individual assistance is available on request from The Learning Centre.

Students are also reminded that careful time management is an important part of study and one of the identified causes of plagiarism is poor time management. Students should allow sufficient time for research, drafting, and the proper referencing of sources in preparing all assessment items.

---

\(^1\)Based on that proposed to the University of Newcastle by the St James Ethics Centre. Used with kind permission from the University of Newcastle

\(^2\)Adapted with kind permission from the University of Melbourne.
Syllabus:

It is not possible to give a week by week schedule of each topic. The topics will be presented in the following order.

1. **Natural Numbers and Integers:**
   - Natural Numbers; Algebraic Properties; Division; Divisibility; Euclid’s Algorithm; Primes.

2. **Representation of Numbers:**
   - Integers; Rationals; Reals; Continued Fractions.

3. **Modular Arithmetic:**
   - Congruences; Divisibility Tests.

4. **Solving Linear Equations:**
   - In Integers; Modulo $n$; Chinese Remainder Theorem.

5. **Powers and Roots:**
   - Fermat’s Theorem; Euler’s Theorem.

6. **Applications:**
   - Arithmetic of Large Numbers; Primality testing; Cryptography; Error-correcting codes.

7. **Polynomials**
   - Arithmetic; common divisors; factorisation; modular arithmetic; Polynomial Equations; Factorising over fields.

8. **Finite Fields:**
   - General Theory; Properties of Finite Fields; Moore’s Theorem; Primitive Elements; Minimal Polynomials.

9. **Error correcting codes:**
   - Hamming codes; BCH codes for one and two errors; general BCH codes.

Course Evaluation and Development:
You will be asked to complete a Course Evaluation for this course some time before the end of Session. These forms, along with any verbal comments you may wish to make, will form the basis for ongoing development of this course and its presentation.

Additional Assessment:
Please refer to the School of Mathematics document “Advice on additional assessment”. Students must adhere strictly to these provisions and be available at the nominated times. *Note that additional assessment will only be granted to students who have achieved at least 40% in their test and assignment and have regularly attended tutorials.*

If you have medical problems or suffer misadventure that means you miss the mid-session test or more than a few lectures and tutorials, then you should contact the lecturer immediately.

For details regarding Additional Assessment see the School of Mathematics Web Page.