Autumn Semester	HG1DMA	Discrete Mathematics and its Applications
Spring Semester	HG12MA	Matrices and their Applications

These two 10-credit modules are independent of each other: you can take either of them without the other. Together, they form a good choice for anyone who wants to do 20 credits of mathematics out of general interest. The prerequisite for HG1DMA is Grade C in Mathematics A-level, but HG12MA requires only Grade C at GCSE.

HG1DMA DISCRETE MATHEMATICS AND ITS APPLICATIONS

MODULE INFORMATION 2007/08

Lecturer: Douglas Woodall
Office: MAPH C120
Phone: (95) 14959
Email: douglas.woodall@nottingham.ac.uk

I am usually in my office, with the door open, from 10.30 to 12.00 and 14.00 to 17.00 each day, except when I am lecturing or otherwise engaged, and you are welcome to drop in whenever my door is open. But to avoid a wasted journey, you may prefer to phone or email me (in plain text, please) to make sure I am there.

Module web pages. The official module web page is accessible through MELEES at

http://www.maths.nottingham.ac.uk/melees/ .

To access this you will need to be officially registered for the module, and to supply your University (Novell) username and password. There is also an unofficial module web page at

http://www.maths.nottingham.ac.uk/personal/drw/DMA/ ,

which is accessible to everyone.

Lectures are on Tuesdays at 11.00 in MAPH C27 and Thursdays at 15.00 in PHARM A5. Friday 14.00 in POPE A21 will be used as a problems class in alternate weeks, starting on Friday 5th October; it will not be used in other weeks (or in the last week of term).

Coursework on this module is set for the purpose of education rather than assessment, and it will not contribute directly to your mark. However, you should regard it as an intrinsic part of the module. It will be set for handing in on alternate Tuesdays, starting on Tuesday 9th October.

Assessment will be by a 2-hour written examination in January. The examination paper will contain six questions, and credit will be given for the best four answers. (This is the same format as the January 2007 exam paper; the 2006 paper was different.) Calculators with a single-line display or dual-line display will be permitted in the examination. Any reassessment will have the same form as the original assessment.

The examination will test your knowledge and understanding of bookwork (i.e., the material written on the board in lectures) and your ability to solve unseen problems based on it. The last two years' examination papers are on the module web page, with solutions and feedback on the 2007 paper. However, the following topics will not be included in the module this year, and so you should ignore the questions cited.

Matrices: 2006 Question 2, 2007 Question 1 and part of Question 3.
The $x^2 - y^2$ method of factorization: 2006 Question 10.
The inclusion-exclusion principle: 2007 Question 5(a).

In contrast, there will be more on cryptography in the module this year.

Provisional syllabus:

1 Graphs and multigraphs

- 1.1 Basic definitions: graphs and multigraphs; isomorphism; degree of a vertex; applications and examples.
- 1.2 Connectedness: walks, trails, paths, cycles; submultigraphs; connected multigraphs, components; cut-vertices and cut-edges (bridges).
- 1.3 Eulerian multigraphs: closed eulerian trails; characterization of eulerian multigraphs; Fleury's algorithm.
- 1.4 Hamiltonian graphs: hamiltonian cycles; Dirac's theorem.
- 1.5 Trees and edge-weighted graphs: trees and forests; the minimal connector problem; the shortest path problem.
- 1.6 Planar graphs: Euler's formula; upper bounds on the number of edges; K_5 and $K_{3,3}$.

2 Counting

- 2.1 Counting rules: addition, multiplication and division rules; sample problems.
- 2.2 Binomial coefficients: definition, simple properties, the binomial theorem.
- 2.3 More counting problems: selections with replacement; multinomial coefficients.

3 Modular arithmetic and cryptography

- 3.1 Modular arithmetic: clock arithmetic; addition, multiplication, powers, inverses.
- 3.2 Classical cryptography: monoalphabetic ciphers (Caesar, affine, keyphrase); polyalphabetic ciphers (Vigenère).
- 3.3 Arithmetic modulo a prime: powers, inverses; Fermat's (little) theorem; the Euclidean algorithm.
- 3.4 Public-key cryptography: RSA, encryption and signed messages.

What you should get out of the module:

Education Aims: Increasingly, communication in business, finance and management is associated with digital processing involving the manipulation and analysis of discrete data. This module introduces some mathematical theory, techniques and algorithms commonly used for display, counting, analysis and manipulation of discrete quantities.

Learning Outcomes:

A student who completes this module successfully should be able to:

Knowledge and understanding

- identify connected graphs;
- identify Euler circuits and Hamiltonian cycles in a graph or else explain their non-existence;
- apply algorithms to determine minimal spanning trees and shortest paths;
- solve various types of counting problems;
- translate 'real world' problems into the language of graph theory and into counting problems and apply or find algorithms to solve them;
- solve simple problems involving integers modulo n;
- recognise the different types of ciphers and apply deciphering techniques;
- use principles of codes and apply some basic constructions.

Intellectual skills

- reason logically and work analytically;
- perform with high levels of accuracy;
- manipulate discrete mathematical structures;
- apply basic mathematical concepts to problems of a routine and extended nature.

Professional skills

- construct and present mathematical arguments with accuracy and clarity.

Transferable skills

- demonstrate skill in problem solving;
- adopt effective strategies for study;
- express ideas and methods of solution in the analysis of mathematical problems appropriately and effectively.

Books. The following books are good introductions, but you will find many others in the same sections of the George Green library, which may be more to your personal taste. There is also the Book of the Module 2006/07, by András Zsak, which is available from the module web page.

R. J. Wilson, *Introduction to Graph Theory* (3rd/4th ed., Longman, 1985/1996, QA91).
R. J. Wilson and J. J. Watkins, *Graphs: an introductory approach: a first course in discrete mathematics* (Wiley, 1990, QA91).
I. Anderson, *A First Course in Combinatorial Mathematics* (2nd ed., Oxford, 1989, QA92).
S. Singh, *The Code Book* (Fourth Estate, London, 1999/2000, QA269.5 in George Green library, or QA76.9.A25 in DLRC, Jubilee Campus).