UNSW Course Outline

ZPEM3301 Topics in Mathematics - 2024

Published on the 11 Feb 2024

General Course Information

Course Code : ZPEM3301
Year : 2024
Term : Semester 1
Teaching Period : Z1
Is a multi-term course? : No
Faculty : UNSW Canberra
Academic Unit : UC Science
Delivery Mode : In Person
Delivery Format : Standard
Delivery Location : UNSW Canberra at ADFA
Campus : UNSW Canberra
Study Level : Undergraduate
Units of Credit : 6

Useful Links

Handbook Class Timetable

Course Details & Outcomes

Course Description

This course introduces a variety of topics in mathematics, including the historical development of mathematics. Topics may be selected from but not limited to the following: classical mechanics; data analysis; calculus of variations; complex variables; projectiles; optimization

techniques; nonlinear dynamical systems theory; industrial mathematics; combinatorics; bush fire modelling; number theory.

Course Aims

The aim of this course is to introduce students to a variety of topics in mathematics, including the historical development of mathematics.

Relationship to Other Courses

This course is an introduction to number theory with a focus on applications to public key cryptography. Everything will be developed from scratch and there are no prerequisites. A familiarity with probability, linear algebra and discrete mathematics will be useful.

Course Learning Outcomes

Course Learning Outcomes
CLO1 : Apply the fundamental concepts (e.g., permutations) and techniques of enumerative combinatorics (e.g., binomial theorem) to count the number of objects for a given scenario.
CLO2 : Construct a combinatoric argument to prove a given result or to provide a count for a particular scenario.
CLO3 : Calculate results using generating functions and recurrence relationships
CLO4 : Utilise analytic and group theoretic techniques in solving combinatorics problems.

Course Learning Outcomes	Assessment Item
CLO1 : Apply the fundamental concepts (e.g., permutations) and techniques of enumerative combinatorics (e.g., binomial theorem) to count the number of objects for a given scenario.	
CLO2 : Construct a combinatoric argument to prove a given result or to provide a count for a particular scenario.	
CLO3 : Calculate results using generating functions and recurrence relationships	
CLO4 : Utilise analytic and group theoretic techniques in solving combinatorics problems.	

Learning and Teaching Technologies

Moodle - Learning Management System

Learning and Teaching in this course

The course makes extensive use of the Moodle on-line learning environment, with weekly slides, lecture recordings, problem sets and solutions, quizzes and supplementary teaching materials all provided online. Please ensure you check Moodle regularly.

Additional Course Information

Public key cryptography forms the foundations of internet security. Number theory, a branch of mathematics which studies properties of the integers such as prime factorization and divisibilit, forms the theoretical foundations of cryptography. This course will introduce students to basic techniques in number theory with a view towards understanding how it is fundamental to cryptography. At the end of the course, students will have a solid understanding of RSA, the Diffie-Hellman key exchange, why these methods of encryption are considered secure and implementation issues which can weaken security.

Assessments

Assessment Structure

Assessment Item	Weight	Relevant Dates
Test 1 Assessment Format: Individual	20%	Start Date: Not Applicable Due Date: Not Applicable
Test 2 Assessment Format: Individual	20%	Start Date: Not Applicable Due Date: Not Applicable
Final exam Assessment Format: Individual	45%	Start Date: Not Applicable Due Date: Not Applicable
Class Work Assessment Format: Individual	15%	Start Date: Not Applicable Due Date: Not Applicable

Assessment Details

Test 1

Assessment Overview

A summative test conducted during the first half of the semester.

Detailed Assessment Description

This test will run for 50 minutes and take place in the final lecture before easter break. It will cover material delieverd throughout the first 5 weeks of lectures, including, but not limited to, prime numbers, modular arithmetic, Diophantine equations and arithmetic functions. Revision Material (including past Examinations and solutions) will also be available on Moodle.

Assessment Length

50 minutes

Assignment submission Turnitin type

This is not a Turnitin assignment

Test 2

Assessment Overview

A summative test covering the later course content.

Detailed Assessment Description

This test will run for 50 minutes and take place in the 11-th week of semester. It will cover material delieverd throughout the second half of semester, including, but not limited to, public key cryptography, primality testing and continued fractions. Revision Material (including past Examinations and solutions) will also be available on Moodle.

Assessment Length

50 minutes

Assignment submission Turnitin type

Not Applicable

Final exam

Assessment Overview

An exam (2 hours). Intended to cover all material and address all CLOs.

Detailed Assessment Description

The Final Examination for this course will be held during the UNSW Canberra Examination Period. Further information about the format and scope of the Final Examination will be provided during class and on Moodle. Revision Material (including past Examinations and solutions) will also be available on Moodle.

Assessment Length

2 hours

Assignment submission Turnitin type

Not Applicable

Class Work

Assessment Overview

The class work assessment item is intended to be formative. It will encompass classroom activities such as, tutorial worksheets and concept discussions. As such it is an on-going assessment item with many hand-in dates. Each aspect of the assessment item addresses at most one CLO but collectively addresses CLO1 & CLO2.

Detailed Assessment Description

The class work component is based on weekly online quizzes posted to moodle at the beginning of each week, starting in the second week. Students will have multiple attempts until the end of the week to submit the quiz via moodle. The topics covered in each quiz will be chosen from the previous week of lecture material.

Assignment submission Turnitin type

Not Applicable

General Assessment Information

Students who have a valid reason for missing a test or quiz (with appropriate certification, eg. a medical certificate) must contact the course convenor within one week of the missed assessment and apply for special consideration so that alternative arrangements can be made.

Missing an assessment without a valid reason will result in a mark of zero for that assessment task.

For information on special consideration refer to https://www.student.unsw.edu.au/special-consideration

It is prohibited to use any software or service to search for or generate information or answers. If its use is detected, it will be regarded as serious academic misconduct and subject to the standard penalties, which may include 00FL, suspension and exclusion.

Grading Basis

Standard

Requirements to pass course

The assessment for the course has been designed so that an overall mark of 50% or greater indicates that the student has unambiguously demonstrated satisfactory completion of each

learning outcome. For this reason, students who receive less than 50% overall for the course will receive a fail grade.

Course Schedule

Teaching Week/Module	Activity Type	Content
Week 1 : 26 February - 1 March	Lecture	Topics: Course outline and introduction, prime numbers, divisibility and the Euclidian algorithm
Week 2 : 4 March - 8 March	Lecture	Topics: The fundamental theorem of arithmetic, modular arithmetic, divisibility testing and algebraic equations
Week 3 : 11 March - 15 March	Lecture	Topics: Systems of modular equations, the Chinese remainder theorem and theorems of Euler, Fermat and Wilson.
Week 4 : 18 March - 22 March	Lecture	Topics: Integer factorization, Euler's function and primality testing.
Week 5 : 25 March - 29 March	Lecture	Topics: Cryptosystems, ciphers and public key cryptography
Week 6 : 1 April - 5 April	Lecture	Topics: Revision and class test
Week 7 : 22 April - 26 April	Lecture	Topics: Ciphers continued, public key cryptography, running time of algorithms.
Week 8 : 29 April - 3 May	Lecture	Topics: Fermat and Euler's theorems revisited, primitive roots, RSA and the Diffie Hellman key exchange.
Week 9 : 6 May - 10 May	Lecture	Topics: Multiplicative functions, multiplicative order and polynomial congruences
Week 10 : 13 May - 17 May	Lecture	Topics: More on primality testing, the Miller-Rabin test and probablistic algorithms
Week 11 : 20 May - 24 May	Lecture	Topics: Continued fractions, rational approximations, revision and class test.
Week 12 : 27 May - 31 May	Lecture	Topics: Applications of continued fractions to encryption, potential security issues with RSA and quadratic residues.
Week 13 : 3 June - 7 June	Lecture	Topics: Quadratic reciprocity and course revision.

Attendance Requirements

Students are strongly encouraged to attend all classes and review lecture recordings.

General Schedule Information

The above Course Schedule is a guide to topics studied each week. For more detailed and up-to-date information regarding the teaching material covered in each class, students should refer to the Course Schedule on the Moodle site for this course. Students need to attend each 2-hour lecture (1500-1700h on Mondays and 1300-1500h on Wednesdays) and 1-hour tutorial (1700-1800h on Mondays) per week. Office hours are by appointment.

Course Resources

Prescribed Resources

Lecture notes will be provided via moodle at the beginning of the semester. Tutorial questions, solutions and supplementary material will be posted on a weekly basis.

Recommended Resources

- Hardy, G. H. and Wright, E. M., *An introduction to the theory of numbers.*, Oxford: Clarendon Press

-Jones, G. A. and Jones, J. M., *Elementary number theory.,* London, England: Springer

Additional Costs

Not Applicable

Staff Details

Position	Name	Email	Location	Phone	Availability	Equitable Learning Services Contact	Primary Contact
Lecturer	Bryce Kerr		Building 26, G23		By appointment	No	Yes

Other Useful Information

Academic Information

Course Evaluation and Development

One of the key priorities in the 2025 Strategy for UNSW is a drive for academic excellence in education. One of the ways of determining how well UNSW is progressing towards this goal is by listening to our own students. Students will be asked to complete the myExperience survey towards the end of each course.

Students can also provide feedback during the semester via: direct contact with the lecturer, the “On-going Student Feedback” link in Moodle, Student-Staff Liaison Committee meetings in schools, informal feedback conducted by staff, and focus groups (where applicable). Student opinions really do make a difference. Refer to the Moodle site for your course to see how the feedback from previous students has contributed to the course development.

Important note: Students are reminded that any feedback provided should be constructive and professional and that they are bound by the Student Code of Conduct.

https://www.gs.unsw.edu.au/policy/documents/studentcodepolicy.pdf

Equitable Learning Services (ELS)

Students living with neurodivergent, physical and/or mental health conditions or caring for someone with these conditions may be eligible for support through the Equitible Learning Services team. Equitable Learning Services is a free and confidential service that provides practical support to ensure your mental or physical health conditions do not adversely affect your studies.

Our team of dedicated **Equitable Learning Facilitators** (ELFs) are here to assist you through this process. We offer a number of services to make your education at UNSW easier and more equitable.

Further information about ELS for currently enrolled students can be found at: https://www.student.unsw.edu.au/equitable-learning

Academic Honesty and Plagarism

UNSW has an ongoing commitment to fostering a culture of learning informed by academic integrity. All UNSW staff and students have a responsibility to adhere to this principle of academic integrity. All students are expected to adhere to UNSW's Student Code of Conduct. Find relevant information at: Student Code of Conduct (unsw.edu.au)

Plagiarism undermines academic integrity and is not tolerated at UNSW. It is defined as using the words or ideas of others and passing them off as your own, and can take many forms, from deliberate cheating to accidental copying from a source without acknowledgement.

For more information, please refer to the following:

https://student.unsw.edu.au/plagiarism

Submission of Assessment Tasks

Special Consideration

Special Consideration is the process for assessing and addressing the impact on students of short-term events, that are beyond the control of the student, and that affect performance in a specific assessment task or tasks.

Applications for Special Consideration will be accepted in the following circumstances only:

- Where academic work has been hampered to a substantial degree by illness or other cause;

- The circumstances are unexpected and beyond the student's control;
- The circumstances could not have reasonably been anticipated, avoided or guarded against by the student; and either:

(i) they occurred during a critical study period and was 3 consecutive days or more duration, or a total of 5 days within the critical study period; or

(ii) they prevented the ability to complete, attend or submit an assessment task for a specific date (e.g. final exam, in class test/quiz, in class presentation)

Applications for Special Consideration must be made as soon as practicable after the problem occurs and at the latest within three working days of the assessment or the period covered by the supporting documentation.

By sitting or submitting the assessment task the student is declaring that they are fit to do so and cannot later apply for Special Consideration (UNSW 'fit to sit or submit' requirement).

Sitting, accessing or submitting an assessment task on the scheduled assessment date, after applying for special consideration, renders the special consideration application void.

Find more information about special consideration at: https://www.student.unsw.edu.au/special/consideration/guide

Or apply for special consideration through your MyUNSW portal.

Late Submission of assessment tasks (other than examinations)

UNSW has a standard late submission penalty of:

- 5% per day,
- capped at five days (120 hours) from the assessment deadline, after which a student cannot submit an assessment, and
- no permitted variation.

Students are expected to manage their time to meet deadlines and to request extensions as early as possible before the deadline.

Electronic submission of assessment

Except where the nature of an assessment task precludes its electronic submission, all assessments must be submitted to an electronic repository, approved by UNSW or the Faculty,

for archiving and subsequent marking and analysis.

Release of final mark

All marks obtained for assessment items during the session are provisional. The final mark as published by the university following the assessment review group meeting is the only official mark.