MA4524: ELEMENTARY NUMBER THEORY AND APPLICATIONS

Effective Term

Semester A 2022/23

Part I Course Overview

Course Title

Elementary Number Theory and Applications

Subject Code

MA - Mathematics

Course Number

4524

Academic Unit

Mathematics (MA)

College/School

College of Science (SI)

Course Duration

One Semester

Credit Units

3

Level

B1, B2, B3, B4 - Bachelor's Degree

Medium of Instruction

English

Medium of Assessment

English

Prerequisites

MA2504 Discrete Mathematics, or
MA2509 Discrete Mathematics

Precursors

Nil

Equivalent Courses

Nil

Exclusive Courses

Nil

Part II Course Details

Abstract

This course introduces basic concepts and knowledge in number theory, together with a wide variety of interesting applications of discrete mathematics. It also trains students to solve problems from algorithm design and analysis, coding theory, Turing machines, etc., and to apply techniques of number theory in cryptography.

Course Intended Learning Outcomes (CILOs)

	CILOs	Weighting (if app.)	DEC-A1	DEC-A2	DEC-A3
1	explain at high levels concepts from elementary number theory, including divisibility and primality.	10	x		
2	state fundamental results in number theory and prove rigorously mathematical statements concerning prime numbers and modular arithmetic.	15	x	x	
3	evaluate greatest common divisors by prime factorizations or Euclid’s algorithm.	15		x	
4	solve linear diophantine equations and linear congruences.	15			x
5	understand properties of common arithmetical functions, including the Euler phi function.	10	x		
6	apply methods and techniques of number theory to a range of applications in cryptography.	15			x
7	the combination of CILOs 1-6	20	x	x	x

A1: Attitude
Develop an attitude of discovery/innovation/creativity, as demonstrated by students possessing a strong sense of curiosity, asking questions actively, challenging assumptions or engaging in inquiry together with teachers.

A2: Ability
Develop the ability/skill needed to discover/innovate/create, as demonstrated by students possessing critical thinking skills to assess ideas, acquiring research skills, synthesizing knowledge across disciplines or applying academic knowledge to real-life problems.

A3: Accomplishments
Demonstrate accomplishment of discovery/innovation/creativity through producing /constructing creative works/new artefacts, effective solutions to real-life problems or new processes.

Teaching and Learning Activities (TLAs)

	TLAs	Brief Description	CILO No.	Hours/week (if applicable)
1	Lectures	Learning through teaching is primarily based on lectures.	1, 2, 3, 4, 5, 6, 7	39 hours in total

2	Take-home assignments	Learning through take-home assignments helps students understand basic results and methods of elementary number theory, as well as the applications of which in algorithm analysis and/or cryptography.	1, 2, 3, 4, 5, 6	after-class

Assessment Tasks / Activities (ATs)

	ATs	CILO No.	Weighting (%)	Remarks (e.g. Parameter for GenAI use)
1	Test	1, 2, 3, 4	15	Questions are designed for the first part of the course to see how well students have learned basic concepts concerning divisibility of integers and prime numbers, as well as methods of solving linear diophantine equations and linear congruences.
2	Hand-in assignments	1, 2, 3, 4, 5, 6	15	These are skills based assessment which enables students to apply basic concepts and techniques of number theory in proving mathematical statements, solving congruences and describing applications in cryptography.
3	Formative take-home assignments	1, 2, 3, 4, 5, 6	0	The assignments provide students chances to demonstrate their achievements on elementary number theory learned in this course.

Continuous Assessment (%)

30

Examination (%)

70

Examination Duration (Hours)

3

Additional Information for ATs

30% Coursework
70% Examination (Duration: 3 hours, at the end of the semester)
For a student to pass the course, at least 30% of the maximum mark for the examination must be obtained.

Assessment Rubrics (AR)

Assessment Task
1. Test

Criterion
Ability in problem solving

Excellent (A+, A, A-)
High

Good (B+, B, B-)
Significant

Fair (C+, C, C-)
Moderate

Marginal (D)
Basic

Failure (F)
Not even reaching marginal levels

Assessment Task
2. Hand-in assignments

Criterion
Understanding of concepts and applications

Excellent (A+, A, A-)
High

Good (B+, B, B-)
Significant

Fair (C+, C, C-)
Moderate

Marginal (D)
Basic

Failure (F)
Not even reaching marginal levels

Assessment Task
3. Formative take-home assignments

Criterion
Study attitude

Excellent (A+, A, A-)
High

Good (B+, B, B-)
Significant

Fair (C+, C, C-)
Moderate

Marginal (D)
Basic

Failure (F)
Not even reaching marginal levels

Assessment Task
4. Examination

Criterion
Comprehensive ability in independent problem solving

Excellent (A+, A, A-)
High

Good (B+, B, B-)
Significant

Fair (C+, C, C-)
Moderate

Marginal (D)
Basic

Failure (F)
Not even reaching marginal levels

Part III Other Information

Keyword Syllabus

The integers, divisibility, primality. GCDs, the Euclidean Algorithm (Complexity). Fundamental Theorem of Arithmetic. Linear Diophantine Equations. Congruences and Modular Arithmetic. Linear Congruences. Chinese Remainder Theorem. Systems of Linear Congruences. Euler’s Theorem. Euler’s Function. Cryptography. Character Ciphers. Block Ciphers. Exponentiation Ciphers. Public-key Cryptosystems.

Reading List

Compulsory Readings

	Title
1	Nil

Additional Readings

	Title
1	Nil