City University of Hong Kong
Course Syllabus

offered by College/School/Department of _Mathematics_____
with effect from Semester __A____ 20_20_ / _21_

Part I Course Overview

Course Title:	**Elementary Number Theory and Applications**
Course Code:	**MA4524**
Course Duration:	**One semester**
Credit Units:	**3 credit units**
Level:	**B4**
Proposed Area: *(for GE courses only)*	☐ **Arts and Humanities** ☐ **Study of Societies, Social and Business Organisations** ☐ **Science and Technology**
Medium of Instruction:	**English**
Medium of Assessment:	**English**
Prerequisites: *(Course Code and Title)*	**MA2504 Discrete Mathematics, or** **MA2509 Discrete Mathematics**
Precursors: *(Course Code and Title)*	**Nil**
Equivalent Courses: *(Course Code and Title)*	**Nil**
Exclusive Courses: *(Course Code and Title)*	**Nil**

Part II Course Details

1. Abstract

(A 150-word description about the course)

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.

2. Course Intended Learning Outcomes (CILOs)

(CILOs state what the student is expected to be able to do at the end of the course according to a given standard of performance.)

No.	CILOs[#]	Weighting* (if applicable)	Discovery-enriched curriculum related learning outcomes (please tick where appropriate)		
			A1	*A2*	*A3*
1.	explain at high levels concepts from elementary number theory, including divisibility and primality.	10%	✓		
2.	state fundamental results in number theory and prove rigorously mathematical statements concerning prime numbers and modular arithmetic.	15%	✓	✓	
3.	evaluate greatest common divisors by prime factorizations or Euclid's algorithm.	15%		✓	
4.	solve linear diophantine equations and linear congruences.	15%			✓
5.	understand properties of common arithmetical functions, including the Euler phi function.	10%	✓		
6.	apply methods and techniques of number theory to a range of applications in cryptography.	15%			✓
7.	the combination of CILOs 1-6	20%	✓	✓	✓
		100%			

** If weighting is assigned to CILOs, they should add up to 100%.*

[#] Please specify the alignment of CILOs to the Gateway Education Programme Intended Learning outcomes (PILOs) in Section A of Annex.

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 self-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.

3. Teaching and Learning Activities (TLAs)

(TLAs designed to facilitate students' achievement of the CILOs.)

TLA	Brief Description	CILO No.							Hours/week (if applicable)
		1	2	3	4	5	6	**7**	
Lectures	Learning through **teaching** is primarily based on lectures.	✓	✓	✓	✓	✓	✓	✓	39 hours in total
Take-home	Learning through **take-home**	✓	✓	✓	✓	✓	✓		after-class

assignments	**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.								

4. Assessment Tasks/Activities (ATs)

(ATs are designed to assess how well the students achieve the CILOs.)

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 Tasks/Activities	CILO No.							Weighting*	Remarks
	1	2	3	4	5	6	7		
Continuous Assessment: _30___%									
Test	✓	✓	✓	✓				15-30%	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.
Hand-in assignments	✓	✓	✓	✓	✓	✓		0-15%	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.
Formative take-home assignments	✓	✓	✓	✓	✓	✓		0%	The assignments provide students chances to demonstrate their achievements on elementary number theory learned in this course.

	Examination: _70___% (duration: 3 hrs, if applicable)		Examination questions are designed to see how far students have achieved their intended learning outcomes. Questions will primarily be skills and understanding based to assess the student's versatility in number theory and its applications.
	** The weightings should add up to 100%.*	100%	

5. Assessment Rubrics

(Grading of student achievements is based on student performance in assessment tasks/activities with the following rubrics.)

Assessment Task	Criterion	Excellent (A+, A, A-)	Good (B+, B, B-)	Fair (C+, C, C-)	Marginal (D)	Failure (F)
1. Test	Ability in problem solving	High	Significant	Moderate	Basic	Not even reaching marginal levels
2. Hand-in assignments	Understanding of concepts and applications	High	Significant	Moderate	Basic	Not even reaching marginal levels
3. Formative take-home assignments	Study attitude	High	Significant	Moderate	Basic	Not even reaching marginal levels
4. Examination	Comprehensive ability in independent problem solving	High	Significant	Moderate	Basic	Not even reaching marginal levels

Part III Other Information (more details can be provided separately in the teaching plan)

1. Keyword Syllabus

(An indication of the key topics of the course.)

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.

2. Reading List

2.1 Compulsory Readings

(Compulsory readings can include books, book chapters, or journal/magazine articles. There are also collections of e-books, e-journals available from the CityU Library.)

1.	
2.	
3.	
…	

2.2 Additional Readings

(Additional references for students to learn to expand their knowledge about the subject.)

1.	
2.	
3.	
…	