Module code	SM-4328			
Module Title	Introduction to Algebra and Number Theory			
Degree/Diploma	Bachelor of Science (Mathematics)			
Type of Module	Major Option			
Modular Credits	4	**Total student Workload**	10	hours/week
		Contact hours	4	hours/week
Prerequisite	SM-2203 Linear Algebra and its Applications			
Anti-requisite	None			

Aims

This module aims to familiarise the student with basic properties of natural numbers and various algebraic structures.

Learning Outcomes

On successful completion of this module, a student will be expected to be able to:

Lower order :	40%	- use the Euclidian and division algorithms and solve linear congruences
Middle order :	40%	-apply certain results of number theory in cryptography
Higher order:	20%	- understand main algebraic structures and use their properties

Module Contents

Method of mathematical induction. Division and Euclidian algorithm.

- Greatest common divisor and least common multiple. Primes and Fundamental Theorem of arithmetics. Congruences and modular arithmetics. Structure of Zn. Solving linear congruences. Chinese Remainder Theorem.
- Fermat Little Theorem. Euler generalization. Public key cryptography.
- Permutations. Order and sign. Cycle decomposition. Definition and examples of groups. Semi-groups. Rings and fields.
- Basic properties of groups. Order of an element. Subgroups. Cyclic groups. Generating sets.
- Cosets. Lagrange Theorem. Fermat and Euler Theorems. Homomorphisms. Normal subgroups.

Assessment	Formative assessment	Tutorial and feedback.
	Summative assessment	Examination: 60%
		Coursework: 40% - 1 class test (20%) - 1 assignment (20%)