



Shanghai Jiao Tong University

MA197 Algebra and Number Theory

Instructor Information:	TBD		
Term:	December 16, 2019 - January 7, 2020	Credits:	4 units
Class Hours :	Monday through Friday, 160 mins per teaching day		
Discussion Sessions:	2 hours each week, conducted by teaching assistant(s)		
Total Contact Hours:	64 contact hours (1 contact hour = 45 mins, 2880 mins in total)		
Required Texts (with ISBN):	Research and Online Learning A Book of Abstract Algebra, by Charles C Printer. ISBN-13: 978-0486474175 ISBN-10: 0486474178 Elements of Number Theory, by John Stillwell ISBN-13: 978-0387942902 ISBN-10: 0387942904		
Prerequisite:	N/A		



Course Overview

Groups in geometry, linear algebra, and number theory; cyclic and abelian groups; permutation groups; subgroups, cosets and normal subgroups; homomorphisms, isomorphisms and the first isomorphism theorem. The Euclidean algorithm, prime factorisation, congruences, the Euler totient function; the theorems of Fermat, Euler and Wilson, and the RSA public key cryptosystem; Chinese remainder theorem; quadratic reciprocity; factorisation and primality testing algorithms.

Learning Outcomes

On completion of this subject students should

1. Appreciate the beauty and the power of pure mathematics;
2. Recognise the fundamental concepts of algebra and number theory;
3. Explain the notion of proof in mathematics and be able to carry out basic proofs;
4. Illustrate how thousands of years of pure mathematical developments have enabled secure electronic communication;
5. Apply important number theoretic algorithms;
6. Describe the power of the generality of the concepts in group theory.



Grading Policy

Ten weekly Assignments	35%
Applied class participation	5%
Middle Exam	20%
Final Exam	40%

Grading Scale

Number grade	Letter grade	GPA
90-100	A	4.0
85-89	A-	3.7
80-84	B+	3.3
75-79	B	3.0
70-74	B-	2.7
67-69	C+	2.3
65-66	C	2.0
62-64	C-	1.7
60-61	D	1.0
≤59	F (Failure)	0



Class Schedule

Date	Lecture	Readings & Assignments
Day 1	Prime factorisation and Euclidean algorithm	Elements of Number Theory
Day 2	Congruence and the Chinese Remainder Theorem	Elements of Number Theory
Day 3	Euler's phi function, Fermat's little theorem	Elements of Number Theory Assignment 1 due (during applied class)
Day 4	Cryptographic applications of number theory	Elements of Number Theory Assignment 2 due (during applied class)
Day 5	Factorisation algorithms, primality testing	Elements of Number Theory Assignment 3 due (during applied class)
Day 6	Quadratic reciprocity	Elements of Number Theory Assignment 4 due (during applied class)
Day 7	Midterm exam	
Day 8	Symmetry and groups	A book of Abstract Algebra Assignment 5 due (during applied class)
Day 9	Introductory group theory	A book of Abstract Algebra Assignment 6 due (during applied class)
Day 10	Examples of groups	A book of Abstract Algebra
Day 11	Examples of groups	A book of Abstract Algebra Assignment 7 due (during applied class)
Day 12	Subgroups	A book of Abstract Algebra Assignment 8 due (during applied class)
Day 13	Lagrange's theorem	A book of Abstract Algebra Assignment 9 due (during applied class)
Day 14	Quotient groups and beyond	Elements of Number Theory Assignment 10 due (during applied class)
Day 15	Final exam	