Shanghai Jiao Tong University

MA197 Algebra and Number Theory

Instructor Information:	Wanchunzi Yu Home Institution: Bridgewater State University Email: wyu@bridgew.edu Office Hours: Determined by Instructor		
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):	A Book of Abstract Algebra, 2nd edition, by Charles C Pinter. ISBN-13: 978-0486474175 ISBN-10: 0486474178 Elements of Number Theory, by John Stillwell ISBN-13: 978-1441930668 ISBN-10: 1441930663		
Prerequisite:	N/A		

Course Overview

This course introduces students to a rigorous study of algebra and number theory. During the first part of the course we will study natural numbers and integers, the Euclidean algorithm, congruence arithmetic, the RSA cryptosystem, quadratic integers, and quadratic reciprocity from the textbook of the Elements of Number Theory. We will learn operations, groups, subgroups, examples of groups and subgroups, as well as quotient groups from a book of abstract algebr

Learning Outcomes

Upon successful completion of this course, students will be conversant with
- understanding concepts of numbers and integers
- the definitions, examples, and applications of groups and subgroups
- developing problem solving skills
- apply concepts and theories to slove problems
- improvements of mathematical thinking skills

Grading Policy

Three Assignments	30%
Quizzes/Attendance	20%
Middle Exam	25%
Final Exam	25%

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	1.1 1.1Natural Numbers 1.2 1.2 Induction 1.3 Integers 1.4 1.4 Division with remainder 1.5 1.5 Binary notation 1.6 1.6 Diophantine equations 1.7 1.7 The Diophantus chord method 1.8 1.8 Gaussian integers 2.1 The gcd by subtraction 2.2 The gcd by division with remainder 2.3 Linear representation of the gcd	Elements of Number Theory Chapter 1 & Chapter 2
Day 2	2.4 Primes and factorization 2.5 Consequences of unique prime factorization 2.6 Linear Diophantine equations 3.1 Congruence mod n 3.2 Congruence classes and their arithmetic 3.3 Inverses mod p	Elements of Number Theory Chapter 2 & Chapter 3
Day 3	3.4 Fermat's little theorem 3.5 Congruence theorems of Wilson and Lagrange 3.6 Inverses mod k 3.7 Quadratic Diophantine equations	Elements of Number Theory Chapter 3
Day 4	4.1 Trapdoor functions 4.2 Ingredients of RSA 4.3 Exponentiation mod n 4.4 RSA encryption and decryption 4.5 Digital signatures 4.6 Other computational issues	Elements of Number Theory Chapter 4
Day 5	7.1 The equation $y^3=x^2+2$ 7.2 The division property in $Z[\sqrt{-2}]$ 7.3 The gcd in $Z[\sqrt{-2}]$ 7.4 $Z[\sqrt{-3}]$ and $Z[\varsigma_3]$	Elements of Number Theory Chapter 7 Assignment 1 due
Day 6	9.1 Primes x^2+y^2, x^2+2y^2, and x^2+3y^2 9.2 Statement of quadratic reciprocity 9.3 Euler's criterion 9.4 The value of $(\frac{2}{q})$ 9.6 The Chinese remainder theorem 9.7 The full Chinese remainder theorem	Elements of Number Theory Chapter 9
Day 7	Chapter 1 Why Abstract Algebra? Chapter 2 Operations	A book of Abstract Algebra
Day 8	Chapter 3 The Definition of Groups	A book of Abstract Algebra

Day 9	Chapter 4 Elementary Properties of Groups	A book of Abstract Algebra Assignment 2 due
Day 10	Chapter 5 Subgroups	A book of Abstract Algebra
Day 11	Chapter 6 Functions Chapter 7 Groups of Permutations	A book of Abstract Algebra
Day 12	Chapter 8 Permutations of a Finite Set Chapter 9 Isomorphism	A book of Abstract Algebra
Day 13	Chapter 15 Quotient Groups & Exam Review	A book of Abstract Algebra Assignment 3 due
Day 14	**Exam 1**	
Day 15	**Exam 2**	