

COURSE SPECIFICATION

The course information as follows may be subject to change, either during the session because of unforeseen circumstances, or following review of the course at the end of the session. Queries about the course should be directed to the course instructor.

1.	Course Title	Elementary Number Theory				
2.	Originating Department	Department of Mathematics				
3.	Course Code	MA209-16				
4.	Credit Value	3				
5.	Course Type	Major Elective Courses				
6.	Semester	Fall				
7.	Teaching Language	English & Chinese				
8.	Instructor(s), Affiliation & Contact For team teaching, please list all instructors	<div style="text-align: center;">3 409</div> <div>huy@sustc.edu.cn</div> <div>0755-8801-5910</div> <div>Yong Hu, Department of Mathematics</div> <div>Block 3, Room 409, Wisdom Valley</div> <div>huy@sustc.edu.cn</div> <div>0755-8801-5910</div>				
9.	Tutor/TA(s), Contact <div style="text-align: center;">/</div>	To be announced				
10.	Maximum Enrolment <div style="text-align: center;">()</div>					
11.	Delivery Method	/ /	/	()		
		Lectures	Tutorials	Lab/Practical	Other Please specify	Total
	Credit Hours	48				48

12. Pre-requisites or Other Academic Requirements	II(MA102a) A (MA102B), II (MA104b)
	Mathematical Analysis II (MA102a) or Advanced Mathematics A II(MA102B), Linear Algebra II (MA104b)
13. Courses for which this course is a pre-requisite	Abstract Algebra
14. Cross-listing Dept.	

SYLLABUS

15. **Course Objectives**

Dirichlet Minkowski

Main topics of the course include basic theories about divisibility, primes, congruences, special Diophantine equations, index and primitive roots, quadratic residues and reciprocity, multiplicative arithmetic functions, Dirichlet series, lattices and Minkowski's theorem, as well as some important applications of number theory. Students are expected to lay down a solid background in number theory, have a feeling of the beauty of the subject, learn about its applications, and get well prepared for subsequent, more advanced courses.

16. **Learning Outcomes**

)

An adequate training through this course should help the students to understand the basic methods and techniques in elementary number theory as well as some important applications. Also, students are expected to have a good understanding of the roles of modern mathematics - including algebra and analysis - in the applications of classical number theoretic questions, thus enhancing their comprehensions of advanced research topics and methods in the frontiers of modern number theory.

17.

Course Contents (in Parts/Chapters/Sections/Weeks. Please notify name of instructor for course section(s), if this is a team teaching or module course.)

(8)

1/2 1

1.1

1.2

1/2 2

2.1

2.2

2.3

2.4

1/2 3 p-

3.1 p-

3.2 n!

1/2 4 Pythagoras

4.1

4.2

4.3

(12h)

1/2 1

1.1

1.2

1/2 2

2.1

2.2

2.3

2.4

2.5

\mathbb{Z}_2^3 _____

3.1

3.2

3.3

(8h)

\mathbb{Z}_2^4 _____

1.1

1.2

\mathbb{Z}_2^5 _____

2.1

2.2

\mathbb{Z}_2^6 _____

3.1

3.2 Carmichael

3.3

(6)

\mathbb{Z}_2^7 _____

\mathbb{Z}_2^8 _____

\mathbb{Z}_2^9 _____

Dirichlet (12)

\mathbb{Z}_2^{10} _____

1.1

1.2 Dirichlet Mobius

\mathbb{Z}_2^{11} Dirichlet _____

2.1 Euler

2.2 Dirichlet L

1/2 3 Dirichlet

3.1 Dirichlet

3.2 Dirichlet L

3.3 Riemann Zeta Riemann

Minkowski (2)

1/2 1 Minkowski

1/2 2 Minkowski

2.1

2.2 Dirichlet

Chapter 1 Divisibility of Integers (8h)

1/2 1 The set of integers and mathematical induction

1.1 The well ordering property and the integral part

1.2 Mathematical induction

1/2 2 Divisibility and prime numbers

2.1 Divisibility of integers

2.2 Representations of integers in different bases

2.3 Greatest common divisor and Euclidean algorithm

2.4 Prime numbers and the fundamental theorem of arithmetic

1/2 3 P-adic valuation of integers

3.1 The p-adic valuation

3.2 Factorization of n!

1/2 4 Pythagorean triples

4.1 Finding solutions with elementary methods

4.2 Rational point on the unit circle

4.3 Fermat's method of infinite descent

Chapter 2 Congruences and Applications (12h)

1/2 1 Introduction to congruences

1.1 Congruences and systems of residues

1.2 Linear congruences

1/2 2 The Chinese Remainder Theorem

2.1 Statement and proof of the theorem

2.2 The ring of congruence classes

2.3 Reduced residue systems

2.4 Some special congruences

2.5 Ring theoretic interpretation of the Chinese remainder theorem

1/2 3 Some applications and complements

3.1 Divisibility tests

3.2 Round-Robin tournaments

3.3 Pseudo primes

Chapter 3 Primitive Roots and Applications (8h)

1/2 1 Order of integers in modular arithmetic

1.1 The order of an integer residue class

1.2 Primitive roots for primes

1/2 2 Numbers having primitive roots

2.1 Prime powers

2.2 The general case

1/2 3 Applications of primitive roots

3.1 Primality tests using orders of integers

3.2 Universal exponents and Carmichael numbers

3.3 Discrete logarithms and power residues

Chapter 4 Quadratic Residues (6h)

1/2 1 Quadratic residues and nonresidues

1/2 2 The law of quadratic reciprocity

1/2 3 An application: Zero-knowledge proof

Chapter 5 Arithmetic Functions and Dirichlet Series (12h)

1/2 1 Arithmetic functions

1.1 Multiplicative functions

1.2 Dirichlet product and Möbius Inversion

1/2 2 Dirichlet series

2.1 Formal series and Euler products

2.2 Dirichlet characters and L-functions

1/2 3 Functions defined by Dirichlet series

3.1 Convergence of Dirichlet series

3.2 Dirichlet L-functions and primes in arithmetic progressions

3.3 Complements on the Riemann zeta function and the Riemann hypothesis

Chapter 6 Lattices and Minkowski's theorem (2h)

1/2 1 Lattice points and Minkowski's theorem

1/2 2 Applications of Minkowski's theorem

2.1 Sums of squares

2.2 Dirichlet's approximation theorem

Textbook:

Kenneth H. ROSEN, Elementary Number Theory and its applications (6th edition) , ISBN-13: 978-0321500311 / ISBN-10: 0321500318

Supplementary Readings:

Tom M. Apostol , Introduction to Analytic Number Theory (Undergraduate Texts in Mathematics) , ISBN-13: 978-1441928054 / ISBN-10: 1441928057

ISBN: 9787301035283

ASSESSMENT

19.

Type of Assessment	Time	% of final score	Penalty	Notes
Attendance				
Class Performance		10		
Quiz				
Projects				
Assignments		20		
Mid-Term Test		35		
Final Exam		35		
Final Presentation				
Others (The above may be modified as necessary)				

20.

GRADING SYSTEM

A.	Letter Grading
B.	/ Pass/Fail Grading

REVIEW AND APPROVAL

21.

/

This Course has been approved by the following person or committee of authority

--