Title (Units): **MATH2630 NUMBER THEORY (3,3,0)** approved by Sci. Board at Oct.18,2011

Course Aims: This course provides an introduction to the theory of numbers. Basic concept such as divisibility, congruence, Diophantine equations will be covered. Some applications such as cryptography will be introduced.

Prerequisite: Year 2 Standing

Instructor: W.C. Shiu

Learning Outcomes (LOs):

Upon successful completion of this course, students should be:

No.	Learning Outcomes (LOs)
	Knowledge
1	Able to understand the divisibility of integers and prime number
2	Able to understand the concept of congruence, modulo, quadratic residues and Chinese remainder theorem
3	Able to understand the properties of some arithmetic functions
4	Able to understand the concept of continued fraction
5	Able to understand the quadratic form and Diophantine equation
6	Able to know the public key cryptography
7	Able to know the distribution of prime numbers
	Skill
8	Able to apply Euclidean algorithm to find the great common divisor, solve system of congruence equations, and system of linear equations
9	Able to apply the continued fractions to approximate an irrational numbers
10	Able to evaluate some classical multiplicative functions and to use of Möbius inversion formula
	Attitudes
11	Able to appreciate the idea of counting and the distribution of primes,
12	Able to apply the knowledge of number theory to solve the real problem

Assessment:

No.	Assessment Methods	Weighting	Remarks
1	Continuous Assessment (assignments and test)	30%	A 1-hour Test and Continuous Assessment are designed to measure how well the students have learned the fundamental concepts and theory.
2	Final Examination	70%	Final Examination questions are designed to see how far students have achieved their intended learning outcomes. Questions will primarily be analysis and skills based to assess the student's versatility in solving congruence equations and Diophantine equations; and finding simple continued fraction of a quadratic algebraic number.

Learning Outcomes and Weighting:

Content	LO No.	Teaching (in hours)
I. Divisibility Properties of Integers	1, 7, 8, 11	4
II. Congruences	2, 8, 12	7
III. Quadratic Reciprocity and Quadratic Forms	3	7
IV. Functions of Number Theory	3, 10, 11, 12	5
V. Diophantine Equations	5, 8, 12	5
VI. Simple Continued Fraction	4, 9, 12	6
VII. Cryptography	6	5

Textbook: K.H. Rosen, Elementary Number Theory, Sixth Ed., Pearson, 2011

References:

G.E. Andrews, Number Theory, Dover, 1994.
D.M. Burton, Elementary Number Theory, McGraw-Hill, 2007.
P. Giblin, Primes and Programming, An Introduction to Number Theory with Computing, Cambridge, 1993.
N. Koblitz, A course in Number Theory and Cryptography, Springer-Verlag, 1987.
W.J. LeVeque, Fundamentals of Number Theory, Dover, 1996.
C.T. Long, Elementary Introduction to Number Theory, Heath and Company, 1972.
I. Niven, H.S. Zuckerman and H.L. Montgomery, An Introduction to The Theory of Numbers, 5th Ed., John Wiley & Sons, 1991.
潘建強 ，邵慰慈：基礎數論，勤達出版社，2008.

Content in Outline:

	Topic	Hours
I.	Divisibility Properties of Integers	4
	A. Divisibility	
	B. Greatest common divisor, Least common multiple, Euclidean algorithm	
	C. Primes, Mersenne primes, Fermat primes, distribution of primes	
II.	Congruences	7
	A. Congruence and congruence equation	
	B. Chinese remainder theorem	
	C. Prime power moduli	
	D. Congruences of degree two	
III.	Quadratic Reciprocity and Quadratic Forms	7
	A. Quadratic residues	
	B. Quadratic reciprocity and Jacobi symbol	
	C. Sums of two squares	
IV.	Functions of Number Theory	5
	A. Arithmetic functions	
	B. Möbius inversion formula	
V.	Diophantine Equations	5
	A. Linear equation	
	B. System of linear equations	
VI.	Simple Continued Fraction	6
	A. Continued fractions	
	B. Approximation to irrational numbers	
	C. Periodic continued fractions, Pell's equation	
VII.	Cryptography	5
	A. Public key cryptography	
	B. RSA cryptosystem	