Detailed Course Description - Course Plan Development and Updating Procedures/ Mathematics Department	QF01/0408-3.0E

Faculty	Faculty of Science and Information Technology	Department	Mathematics
Course number	0101212	Course title	Number Theory
Number of credit hours	3	Pre-requisite/co-requisite	Set Theory 0101211

Brief course description
Properties of Integer Numbers, Division Algorithm, Greatest Common Divisor, Least Common Multiple, Prime Numbers, Fundamental Theorem Of Arithmetic, Congruence, Linear Congruence, Chinese Remainder Theorem, Fermat's Theorem, Welson's Theorem and Diophantine Equations.

	Course goals and learning outcomes
Goal 1	To introduce and provide students with a good understanding of the basic concepts in number theory.
Learning outcomes	1.1 Student will be able to define and interpret the concepts of divisibility, congruence, greatest common divisor, prime, and prime-factorization. 1.2 Student will be able to collect and use numerical data to form conjectures about the integers. 1.3 Student will be able to understand the concept of a congruence and use various results related to congruences including the Chinese Remainder Theorem. 1.4 Use appropriate technological tools while solving mathematical problems.
Goal 2	To help students develop the ability to prove theorems and solve problems.
Learning outcomes	2.1 Student will be able to effectively express the concepts and results of Number Theory. 2.2 Student will be able to understand the logic and methods behind the major proofs in Number Theory and to solve challenging problems in Number Theory. 2.3 Student will be able to produce rigorous arguments (proofs) centered on the material of number theory, most notably in the use of Mathematical Induction and/or the Well Ordering Principal in the proof of theorems. 2.4 Students will gain experience and confidence in proving theorems. 2.5 Construct correct logical arguments and understand and critique the reasoning of others.
Goal 3	Present applications of number theory, which may include cryptology
Learning outcomes	3.1 Student will be able to apply theoretical knowledge to problems in computer security. 3.2 Be able to apply physical insight and mathematical techniques to the solution of problems in applied mathematics.

1. Elementary Number Theory. By: Strayer	الكتاب المعتمد: (Text Book)
1) Elementary Number Theory. By: David M. Burton	المراجع العلمية: (References)
2) Number Theory and its application. By: Kenneth H. Rosen.	
3) Number Theory and its history. By: Oystein ore.	
4) Number Theory: an Introduction. By: D. Redmond.	

Week	Number of hours	Course timeline	الصفحات في الكتاب المعتمد	Notes
01	1 1 1	Divisibility with properties, the division algorithm theorem (state and proof) with applications	3 – 11	
02	1 1 1	The division algorithm theorem (state and proof) with applications. Prime and composite numbers.	3 – 11	
03	1 1 1	Prime and composite numbers. There are infinitely many prime numbers. If n is any composite number, then n has a prime divisor p with $p \leq \sqrt{n}$.	11 – 18	
04	1 1 1	Mersenne prime twin prime and Fermat prime. The greatest common divisor and the meaning of relatively primes.	11 – 18	
05	1 1 1	The G.C.D. The G.C.D (a,b) as a linear combination of a and b.	18 – 26	
06	1 1 1	The G.C.D by using Euclidean algorithm. [First Exam 20%]	18 – 26	
07	1 1 1	Theorem of prime numbers. State and prove the fundamental theorem of arithmetic.	26 – 29	
08	1 1 1	(a,b) [a,b] = ab among other statements. We prove that a divides b if, and only if a^2 divides b^2.	29 – 37	
09	1 1 1	Congruence's. congruence modulo m is an equivalence relation on z. def. of a complete residue. system modulo m.	38 – 43	
10	1 1 1	If $a \equiv b \bmod (m)$ and $c \equiv d \bmod (m)$,then $a+c \equiv b+d \bmod (m)$ and $ac \equiv bd \bmod (m)$ The set of equivalence classes modulo 4 is denoted by $z_4 = \{ [0],[1],[2],[3] \}$.	43 – 48	

11	1 1 1	Ca ≡ Cb mod (m) if, and only if a ≡ b mod (m/(c,m). the linear congruence in one variable	48 – 54	
12	1 1 1	the multiplicative inverse of a modulo m, all incongruent solutions of ax ≡ b mod(m), if it exists. [Second Exam 20%]	48 – 54	
13	1 1 1	The Chinese remainder theorem , solve the system of congruence's such as 2x ≡ 1 mod(3) 3x ≡ 2mod(5) and 5x ≡ 4mod(7).	54 – 59	
14	1 1 1	Wilsons theorem and Fermat's little theorem and showing that $a^p \equiv a \bmod(p)$.	59 – 68	
15	1 1 1	Euler phi- function and Euler's theorem. Finding all incongruent solutions.	68 – 75	
16	1 1 1	[Final Exam 50%]	-	

Theoretical course evaluation methods and weight	Participation = 10% First exam 20% Second exam 20% Final exam 50%	**Practical (clinical) course evaluation methods**	Semester students' work = 50% (Reports, research, quizzes, etc.) Final exam = 50%

Approved by head of department		**Date of approval**	

Extra information (to be updated every semester by corresponding faculty member)

Name of teacher	Hamza Alzaareer	Office Number	**9130**
Phone number (extension)	423	Email	**h.alzaareer@zuj.edu.jo**
Office hours			