JARAMOGI OGINGA ODINGA UNIVERSITY OF SCIENCE AND TECHNOLOGY

SCHOOL OF MATHEMATICS AND ACTUARIAL SCIENCE

UNIVERSITY EXAMINATION FOR DEGREE OF BACHELOR OF SCIENCE, BIS, ICT, COMPUTER SECURITY

2ND YEAR 1ST SEMESTER 2015/2016 ACADEMIC YEAR

REGULAR

COURSE CODE: IIT 3218

COURSE TITLE: INTRODUCTION TO NUMBER THEORY

EXAM VENUE: **STREAM: (BSc. Actuarial)**

DATE: EXAM SESSION:

TIME: 2.00 HOURS

Instructions:

1. **Answer question 1 (Compulsory) and ANY other 2 questions**
2. **Candidates are advised not to write on the question paper.**
3. **Candidates must hand in their answer booklets to the invigilator while in the examination room.**

QUESTION ONE (Compulsory) [30 Marks]

(a) State carefully the following principles as used in number theory: [3 mks]

(i) the well-ordering principle

(ii) the pigeonhole principle

(iii) the principle of mathematical induction

(b) Find the base 3 expansion of $(593)_7$. [3 mks]

(c) If a, b, & c are integers such that a divides b, and b divides c, show that a divides c. [3 mks]

(d) Write the following integers 11 and 7983 as congruence modulo 8 [2 mks]

(e) Use the Sieve of Aratosthenes to find all primes less than 100. [3 mks]

(f) Define the Euler ϕ-function of a positive integer n, $\phi(n)$, and hence find $\phi(4)$ and $\phi(16)$. [4 mks]

(g) If a and b are integers both of the form $4n+1$, show that their product ab is also of the form $4n+1$. [3 mks]

(h) Give a set of 5 integers that are both mutually relatively prime as well as pairwise relatively prime. [2 mks]

(i) Find all the solutions of the congruence $3x \equiv 12 (mod\, 6)$. [4 mks]

(j) Let a and b be two real numbers. Prove that

$$\min(a,b) + \max(a,b) = a + b$$

where $\min(a,b)$ and $\max(a,b)$ are respectively the minimum and maximum of the numbers a and b. [3 mks]

QUESTION TWO [20 Marks]

(a) Use the principle of mathematical induction to prove that

$$n! \leq n^n$$

for each $n \in \mathbb{N}$. [6 mks]

(b) Let (a, b) denotes the greatest common divisor (GCD) of the integers a and b. Show that if $(a, b) = d$, then $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$. [6 mks]

(c) By using the Euclidean algorithm, find the GCD of the integers 4147 & 10672, and hence express the GCD as a linear combination of 4147 & 10672. [8 mks]

QUESTION THREE [20 Marks]

(a) If n is a composite integer, show that n has a prime factor not exceeding $\sqrt{n}$. [5 mks]

(b) Prove that there are infinitely many primes. [6 mks]

(c) Let the prime factorization of the integers a and b be given by $a = p_1^{a_1} p_2^{a_2} \cdots p_m^{a_m}$ and $b = p_1^{b_1} p_2^{b_2} \cdots p_m^{b_m}$.

(i) Define the least common multiple (LCM) and the greatest common divisor (GCD) of a and b in terms of the prime factorization. [2 mks]

(ii) Show that $\langle a, b \rangle = \frac{ab}{(a,b)}$, where $\langle a, b \rangle$ and (a, b) are respectively, the LCM and the GCD of a, b. [5 mks]

QUESTION FOUR [20 Marks]

(a) Convert $(AB6C7D)_{16}$ to binary notation if $A = 10$, $B = 11$, $C = 12$ and $D = 13$. [6 mks]

(b) Prove that if $a \equiv b (mod\, m)$ and $b \equiv c (mod\, m)$, then $a \equiv c (mod\, m)$. [4 mks]

(c) Define the following terms and give an example of each: [5 mks]

(i) A complete residue system modulo m

(ii) A reduced residue system modulo m

(d) Briefly describe **Cryptography** as an application of number theory. [4 mks]

QUESTION FIVE [20 Marks]

(a) State the Chinese Remainder Theorem. [2 mks]

(b) Solve the following system of congruences: [8 mks]

$$\begin{aligned} x &\equiv 1(mod\, 2) \\ x &\equiv 2(mod\, 3) \\ x &\equiv 3(mod\, 5). \end{aligned}$$

(c) Find all the integers that leave a remainder of 1 when divided by 2, a remainder of 2 when divided by 3, and a remainder of 3 when divided by 5. [5 mks]

(d) Define the function $f(x) = [x]$, and sketch its graph. [5 mks]