MACHAKOS UNIVERSITY

University Examinations for 2020/2021

SCHOOL OF PURE AND APPLIED SCIENCES

DEPARTMENT OF MATHEMATICS AND STATISTICS

THIRD YEAR FIRST SEMESTER EXAMINATION FOR

BACHELOR OF SCIENCE (STATISTICS AND PROGRAMMING)

BACHELOR OF EDUCATION (SCIENCE)

SMA 304: NUMBER THEORY

DATE: 9/8/2021 **TIME: 8:30 – 10:30 AM**

INSTRUCTION: *Answer Question* ***ONE*** *which is compulsory and any other* ***TWO*** *Questions*

QUESTION ONE (COMPULSORY) (30 MARKS)

a) Let m be a fixed positive integer. Using appropriate examples, distinguish between the meaning of the term *congruence modulo* m and the term *reduced residue modulo* m. (5 marks)

b) Assume that a and b are positive integers satisfying $a > b$. Is it possible to find a positive integer $c < b$ such that b is congruent to c modulo a? Justify your Answer. (5 marks)

c) Let x and y be non-zero integers and z be any integer. Show that if $x \mid 17331y$ and $y \mid z$ then $x \mid 641247z$. (5 marks)

d) Let $a \in \mathbb{Z}$ and $b_1, b_2, \dots, b_n$ be a sequence of integers such that $a \mid b_i$ for each $i = 1,2, \dots, n$. Prove that

$$a \mid (b_1y_1 - b_2y_2 - \cdots - b_ny_n)$$

for any $y_1, y_2, \dots, y_n \in \mathbb{Z}$. (5 marks)

e) Prove that if q is an odd integer then $q^2 = 8k + 1$ for some $k \in \mathbb{Z}$ (5 marks)

f) Express the following pairs of integers in the form $a = bq + r$ with $0 \le r < b$

(i) $a = -3561, b = 98,$ (3 marks)

(ii) $a = 337, b = 751.$ (2 marks)

QUESTION TWO (20 MARKS)

a) Given that a, b are non zero integers, prove that $a \mid b$ and $b \mid a$ if and only if $a = \pm b$.

(5 marks)

b) Let $m \in \mathbb{Z}$. Prove that either $m^2 = 4k$ or $m^2 = 4k + 1$ for some integer k. (4 marks)

c) Use the Euclidean algorithm

(i) to find $d = \gcd(2327,819)$, (3 marks)

(ii) express $\gcd(2327,819)$ in the form $d = 2327x + 819y$. (3 marks)

d) Let x, y, m be integers with $m > 0$. Prove that if $x \equiv y (\text{mod } m)$ then $x^n \equiv y^n (\text{mod } m)$ for any positive integer n. (5 marks)

QUESTION THREE (20 MARKS)

a) In your own words, distinguish between *prime* numbers and *relatively prime* numbers. (2 marks)

b) Let a, b, m be integers with $m > 0$ and suppose that $a \equiv b(mod \quad m)$.

(i) Prove that $a - x \equiv b - x(mod \quad m)$ for any integer x. (4 marks)

(ii) Solve the linear congruence $506x + 6 \equiv 29(mod 391)$ (5 marks)

c) Prove that if m is an integer then $3 \mid (m^3 - m)$. (5 marks)

d) Construct at least two distinct complete residue systems modulo 6. For each of the given complete residue systems, determine their corresponding reduced residue systems modulo 6. (4 marks)

QUESTION FOUR (20 MARKS)

a) Suppose that a, b are non-zero integers such that $a = bq + r$ for some integers q, r. Prove that if $d = \gcd(b, r)$ then $d \mid a$. (7 marks)

b) Suppose that $a \in \mathbb{Z}$ is a positive integer greater than 1. Prove that the number $\frac{a^3+5a}{3}$ is an integer. (6 marks)

c) Suppose that a, b are non-zero integers. Prove that $\gcd(6a - 9b, 9a - 13b) \mid b$. Hence or otherwise show that $\gcd(6a - 9,9a - 13) = 1$ for any integer a. (7 marks)

QUESTION FIVE (20 MARKS)

a) Use examples and elaborate in your own words what you understand by the following terms

(i) a *linear diophantine* equation, (2 marks)

(ii) a pair of *relatively prime* numbers. (2 marks)

b) Prove that the number $n(n+1)(2n+1)$ is divisible by 6. (5 marks)

c) Let a, b, c, d, m be non-zero integers with $m > 0$. Suppose that $a \equiv b(\text{mod } m)$ and $c \equiv d(\text{mod } m)$. Prove that

(i) $ax - c \equiv bx - d(\text{mod } m)$ for any integer x, (3 marks)

(ii) $ac \equiv bd(\text{mod } m)$. (3 marks)

d) Solve the following linear Diophantine Equations (5 marks)

(i) $111x + 321y = 690$

(ii) $54x + 21y = 91$