MACHAKOS UNIVERSITY

University Examinations 2019/2020 Academic Year

SCHOOL OF PURE AND APPLIED SCIENCES

DEPARTMENT OF MATHEMATICS AND STATISTICS

THIRD YEAR SPECIAL /SUPPLEMENTARY EXAMINATION FOR

BACHELOR OF SCIENCE IN MATHEMATICS

SMA 304: NUMBER THEORY

DATE: 18/01/2021 **TIME: 2.00-4.00 PM**

INSTRUCTIONS TO CANDIDATES

Answer Question One and any other two questions

QUESTION ONE (30 MARKS)

a) Let m be a fixed positive integer. Explain the meaning of the following terms

i. *congruence modulo* m, (2 marks)

ii. *reduced residue modulo* m. (2 marks)

b) Prove that the product of two odd numbers is an odd number. (4 marks)

c) Let x, y and z be integers. Show that if $x|y$ and $y|z$ then $x|z$. (4 marks)

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

$$a|(b_1y_1 + b_2y_2 + \cdots + b_ny_n)$$

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

e) Let $x, y, z \in \mathbb{Z}$. Prove that if m is any positive integer then:

i. $x \equiv x(\text{mod } m)$, (2 marks)

ii. if $x \equiv y(\text{mod } m)$ then $y \equiv x(\text{mod } m)$ and (3 marks)

iii. if $x \equiv y(\text{mod } m)$ and $y \equiv z(\text{mod } m)$ then $x \equiv z(\text{mod } m)$. (3 marks)

f) Let $a \in \mathbb{Z}$ be any integer. Verify that $3|a(2a^2 + 7)$. (5 marks)

QUESTION TWO (20 MARKS)

(a) Given that a, b are non zero integers, prove that $a|b$ and $b|a$ 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 a, b, m be integers with $m > 0$. Prove that if $a \equiv b(mod\ m)$ then $a^n \equiv b^n(mod\ m)$ for any positive integer n. (5 marks)

QUESTION THREE (20 MARKS)

a) Distinguish between *prime* numbers and *relatively prime* numbers. (2 marks)

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

(i) Prove that $a - x \equiv b - x(mod\ m)$ 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 $3\ |(m^3 - m)$. (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.

i. Explain the meaning of the term *a greatest common divisor* of a and b. (2 marks)

ii. Suppose that $a = bq + r$ for some integers a, r. Prove that $gcd(a, b) = gcd(b, r)$ (5 marks)

b) Suppose that $a \in \mathbb{Z}$ is a positive integer greater than 1. Prove that the number $a(a^2 + 2)$ is divisible by 3. (6 marks)

c) Suppose that a, b are non-zero integers. Prove that

$$gcd(6a - 9b, 9a - 13b)|b.$$

Hence or otherwise show that $gcd(6a - 9,9a - 13) = 1$ for any integer a. (7 marks)

QUESTION FIVE (20 MARKS)

a) Explain the meaning of 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 $a \equiv b(mod\ m)$ and $c \equiv d(mod\ m)$. Prove that

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

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

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

i. $111x + 321y = 690$

ii. $54x + 21y = 91$