MACHAKOS UNIVERSITY

University Examinations for 2024/2025 Academic Year

SCHOOL OF PURE AND APPLIED SCIENCES
DEPARTMENT OF MATHEMATICS, STATISTICS AND ACTUARIAL SCIENCES

THIRD YEAR FIRST SEMESTER EXAMINATION FOR DEGREE IN
BACHELOR OF SCIENCE IN MATHEMATICS
BACHELOR OF SCIENCE IN MATHEMATICS AND COMPUTER SCIENCE
BACHELOR OF SCIENCE IN STATISTICS AND PROGRAMMING
BACHELOR OF EDUCATION (SCIENCE)

SMA 304: NUMBER THEORY

DATE: 21ST JANUARY, 2025 **TIME: 8.30 AM- 10.30 AM**

INSTRUCTIONS:
*Answer question **ONE (Compulsory)** and **any other TWO** questions*

QUESTION ONE *(COMPULSORY)* (30 MARKS)

(a) State the *well ordering principle* of non-negative integers. **(2 Marks)**

(b) Let $a, b, c \in \mathbb{Z}$. Show that if $a|b$ and $b|c$ then $a|c$. **(3 Marks)**

(c) Let $a, b_1, b_2, \ldots, b_n \in \mathbb{Z}$ be such that $a|b_i$ for each $i = 1,2, \ldots, n$. Prove that

$$a|(b_1x_1 + b_2x_2 + \cdots + b_nx_n)$$

for any $x_1, x_2, \ldots, x_n \in \mathbb{Z}$. **(5 Marks)**

(d) Use the extended division algorithm to calculate the greatest common divisor of $a = 51684$ and $b = 6950$. **(5 Marks)**

(e) Solve the following linear Diophantine Equations **(5 Marks)**

(i) $26x + 39y = 91$

(ii) $112x + 36y = 73$

(f) Solve the linear congruence equation $231x = 189 (\text{mod } 357)$. **(5 Marks)**

(g) Let $a \in \mathbb{Z}$ be any integer. Prove that $a(2a^2 + 7)$ is divisible by 3. **(5 Marks)**

QUESTION TWO - (20 MARKS)

(a) Let $r \in \mathbb{Z}$. Prove that either $r^2 = 4s$ or $r^2 = 4s + 1$ for some integer s. **(4 Marks)**

(b) Explain the meaning of the *Euler ϕ-function* of a positive integer n hence or otherwise determine $\phi(22)$. **(5 Marks)**

(c) Suppose that $q \in \mathbb{Z}$ is a positive integer greater than 1. Prove that **(6 Marks)**

$$\frac{q(q^2 + 3)}{3} \text{ is an integer.}$$

(d) Suppose that a, b are non-zero integers. Prove that **(5 Marks)**

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

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

QUESTION THREE - (20 MARKS)

(a) Explain the meaning of the following terms: **(3 Marks)**

(i) *residue system modulo n*,

(ii) *reduced residue system modulo n.*

(b) Prove that if u is an odd integer then $u^2 = 8v + 1$ for some $v \in \mathbb{Z}$. **(5 Marks)**

(c) Let $a, b \in \mathbb{Z}$. Show that if $a|b$ then $a|bc$ for any $c \in \mathbb{Z}$. **(2 Marks)**

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

(5 Marks)

(i) $a = -3291, b = 112$,

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

(e) Solve the Diophantine equation $7171x + 7952y = 2627$. **(5 Marks)**

QUESTION FOUR - (20 MARKS)

(a) Let m be a fixed positive integer. Explain the meaning of *congruence modulo* m.

(2 Marks)

(b) Suppose that x, y, z, w are non-zero integers. Show that if $x|z$ and $y|w$ then $xy|zw$.

(3 Marks)

(c) Let $x, y, z \in \mathbb{Z}$. Prove that if m is any positive integer then: **(6 Marks)**

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

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

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

(d) State the Division Algorithm. **(3 Marks)**

(e) Let $d = gcd(7623,818)$. Determine the integers x, y such that $d = 7623x + 818y$.

(6 Marks)

QUESTION FIVE - (20 MARKS)

(a) Distinguish between *prime* numbers and *relatively prime* numbers. **(3 Marks)**

(b) Prove that if m is an integer then $3|(m^3 - m)$. **(5 Marks)**

(c) Construct at least two distinct complete residue systems modulo 9. For each of the given complete residue systems determine their corresponding reduced residue systems modulo 9. **(6 Marks)**

(d) Prove that if a is an integer neither divisible by 2 nor 3 then $a^2 \equiv 1 (\text{mod } 24)$.

(6 Marks)