HAL-003-1163003

Seat No. _______________

HAL-003-1163003

M. Sc. (Sem. III) (CBCS) Examination

June – 2023

Mathematics

(Number Theory 1)

Faculty Code : 003
Subject Code : 1163003

Time : $2\frac{1}{2}$ Hours / Total Marks : **70**

Instructions :

(1) There are five questions.
(2) All questions are compulsory.
(3) Each question carries 14 marks.

1 Do as directed : (Answer any **seven**) **7×2=14**

(a) If we consider any integer a in modulo 3 system then show that $\frac{a(a^2+3)}{3}$ is an integer.

(b) Prove that g.c.d of any two integers is always positive.

(c) Prove that $[ga, gb] = g \cdot [a, b]; \forall a, b \in \mathbb{Z} - \{0\}$, for $g > 0$.

(d) Find the $g.c.d$ of $(5a+2, 7a+3); \forall a \in \mathbb{Z}$.

(e) Define : (i) L.C.M. and (ii) Order of an element.

(f) Define Reduced Residue System in modulo m with an example.

(g) Define (i) Totally Multiplicative Function and (ii) Primitive Root.

(h) Find all solutions of $3x \equiv 6 \pmod 9$ if exists.

(i) Find the number of solution of $x^2 \equiv -1 \pmod{11}$.

(j) If $a = 2m+1$, then show that $a^2 \cong 1 \pmod 8$.

2 Answer any **two** of the following : **2×7=14**

(a) Prove that if order of $a(\mathrm{mod}\, m)$ is h then for any integer $j \geq 1$ order of $a^j(\mathrm{mod}\, m) = \dfrac{h}{(h, j)}$.

(b) Prove that there are infinitely prime numbers.

(c) If $m, m_1, m_2 \geq 1$ with $1 = (m_1, m_2)$ and $m = m_1 \cdot m_2$ then prove that the number of solutions of $f(x) \cong 0(\mathrm{mod}\, m)$ is equal to the product of the number of solutions of $f(x) \cong 0(\mathrm{mod}\, m_1)$ and $f(x) \cong 0(\mathrm{mod}\, m_2)$.

3 Answer the following : **2×7=14**

(a) State and Prove fundamental theorem of arithmetic.

(b) Prove that if p is a prime number then p^2 has exactly $(p-1)\varnothing(p-1)$ primitive roots in $(\mathrm{mod}\, p^2)$.

OR

3 Answer the following : **2×7=14**

(a) State and Prove Enclid's Algorithm.

(b) State and Prove Chinese Remainder Theorem.

4 Answer the following : **2×7=14**

(a) State and prove any five properties of divisibility.

(b) (i) State and Prove Fermat's Theorem. **3**

(ii) If p is a prime number of the form $4k+3$ and $p \mid a^2 + b^2$ then $p \mid a$ and $p \mid b$ for some $a, b \in \mathbb{Z}$. **4**

5 Answer any **two** of the following : **2×7=14**

(a) State and prove Mobius Inversion Formulae.

(b) State and prove Wilson's Theorem.

(c) Prove the every *g.c.d.* can be expressed as a linear combination of given two integers a and b and vice-versa.

(d) (i) Prove that $[a, b] \cdot (a, b) = |a.b|$ **5**

(ii) If $a \mid c$ and $b \mid c$ with $(a, b) = 1$ then show that $ab \mid c$. **2**