UUCMS NO

B.M.S COLLEGE FOR WOMEN AUTONOMOUS

BENGALURU -560004

END SEMESTER EXAMINATION – APRIL/ MAY 2023

M.Sc. Mathematics – I Semester
ELEMENTARY NUMBER THEORY

Course Code MM107S **QP Code: 11006**
Duration : 3 Hours **Maximum Marks: 70**

Instructions: 1) **All** questions carry **equal** marks.
2) Answer **any five** full questions.

1. (a) State and prove division algorithm.
   (b) Determine all solutions in the set of integers of the diophantine equation
   $172x + 20y = 1000.$ **(7+7)**

2. (a) State and prove fundamental theorem of arithmetic.
   (b) If the square root of a positive integer m is rational, show that m is a perfect square. **(7+7)**

3. (a) Show that $a \equiv b\ (mod\ m)$ if and only if $ac \equiv bc\ (mod\ m)$ for any $c > 0$.
   (b) State and prove Euler-Fermat theorem.
   (c) Find all the positive integers n for which $n^{17} \equiv n\ (mod\ 4080)$. **(4+4+6)**

4. (a) State and prove Lagrange's theorem for polynomial congruences $mod\ p$.
   (b) Solve the simultaneous congruences:
   (i) $x \equiv 1\ (mod\ 3)$
   $x \equiv 2\ (mod\ 4)$
   $x \equiv 3\ (mod\ 5)$
   (ii) $x^2 + 2x + 2 \equiv 0\ (mod\ 5)$
   $7x \equiv 3\ (mod\ 11)$ **(7+7)**

5. (a) If p is an odd prime, prove that every reduced residue system $mod\ p$ contains exactly $\frac{p-1}{2}$ quadratic residues and exactly $\frac{p-1}{2}$ quadratic non-residues $mod\ p$. Also show that the quadratic residues belong to the residue classes containing the numbers $1^2, 2^2, 3^2, \dots, \left(\frac{p-1}{2}\right)^2$.
   (b) Define Legendre symbol $\left(n/p\right)$. Prove that the Legendre symbol $\left(n/p\right)$ is a completely multiplicative function of n.
   (c) Evaluate the Legendre symbol $\left(11/23\right)$ using Gauss lemma. **(6+5+3)**

6. (a) If p is an odd prime, show that that $\sum_{r=1}^{p-1} r\left({}^{r}/_{p}\right) = 0$ if $p \equiv 1\ (mod\ 4)$.
(b)If P and Q are odd positive integers such that $(P, Q) = 1$, prove that
$\left({}^{P}/_{Q}\right)\left({}^{Q}/_{P}\right) = (-1)^{\frac{(P-1)(Q-1)}{4}}$.
(c)If p is an odd prime and $(a, p) = 1$, prove that the diophantine equation $x^2 + py + a = 0$ has an integral solution if and only if $\left({}^{-a}/_{p}\right) = 1$. **(5+5+4)**

7. (a) If p is a prime and $(a, p) = 1$, prove that the linear congruence $ax \equiv y\ (mod\ p)$ has a solution (x_0, y_0), where $0 < |x_0| < \sqrt{p}$ and $0 < |y_0| < \sqrt{p}$
(b) Show that any prime p of the form $4k + 1$ can be represented uniquely as a sum of two squares.
(c) Express 6409 as a sum of two squares. **(5+7+2)**

8. (a) Prove that any prime p can be expressed as the sum of four squares.
(b) Show that all the solutions of the Pythagorean equation $x^2 + y^2 = z^2$ satisfying the conditions $(x, y, z) = 1, {}^{2}/_{x}, x > 0, y > 0, z > 0$ are given by $x = 2st, y = s^2 - t^2, z = s^2 + t^2$ for integers $s > t > 0$ such that $(s, t) = 1$ and $s \not\equiv t\ (mod\ 2)$.
(7+7)

****