Registration No.: | | | | | | | | | | |

Total Number of Pages: 02

Course: M.Sc.I
Sub Code: FMCC502

5th Semester Regular Examination: 2024-25
SUBJECT: Number Theory
BRANCH(S): M.Sc.I(MC)
Time: 3 Hours
Max Marks: 70
Q.Code: R257
Answer Question No.1 (Part-I) which is compulsory, any five from rest (Part-II)
The figures in the right-hand margin indicate marks.

Part-I

Q1 Answer the following questions: **(2 x 10)**

- **a)** Find the number of positive integers ≤ 3000 and divisible by $3, 5$, or 7.
- **b)** Prove that there are infinitely many primes.
- **c)** Show that $11 \times 14^n + 1$ is a composite number.
- **d)** On what day of the week will January 14, 2020, occur?
- **e)** Show that the Euler phi-function $\phi(n)$ is an even integer for $n \geq 2$.
- **f)** Find the index of 5 relative to each of the primitive roots of 13.
- **g)** Show that the Fermat number F_5 is divisible by 641.
- **h)** Verify that the Mersenne number M_{11} is a composite number.
- **i)** Obtain all primitive Pythagorean triples x, y, z in which $x = 40$.
- **j)** Write 15795 as the sum of four squares.

..

Part-II

Long Answer Type Questions (Answer Any five)

Q2 **a)** Prove that every integer $n > 1$ either is a prime or can be expressed as a product of primes in only one way apart from the order of the factors. Also, prove that the factorization into primes is unique except for the order of the factors. **(5+5)**

b) Using Chinese remainder theorem, solve the system of congruence:

$$x \equiv 5 \ mod(6)$$
$$x \equiv 4 \ mod(11)$$
$$x \equiv 3 \ mod(17).$$

Q3 **a)** Prove that the linear Diophantine equation $ax + by = c$ is solvable if and only if $d|c$, where $d = gcd(a, b)$. Also prove if (x_0, y_0) is any particular solution of this equation, then all its solutions are given by $x = x_0 + (b/d)t$ and $y = y_0 - (a/d)t$. **(5+5)**

b) Find the solutions of the system of congruences:

$$7x + 3y \equiv 10 \ mod(16)$$
$$2x + 5y \equiv 9 \ mod\ (16).$$

Q4 **a)** Prove that if $n \geq 1$ and $gcd(a,n) = 1$, then $a^{\phi(n)} \equiv 1 \, mod \, (n)$. **(5+5)**

b) Show that if the integer a has order k modulo n and $h > 0$, then a^h has order $\frac{k}{\text{gcd}\,(h,k)}$ modulo n.

Q5 **a)** State and prove Wilson's theorem. **(5+5)**

b) Show that if $gcd(m,n) = 1$, where $m > 2$ and $n > 2$, then the integer mn has no primitive roots.

Q6 **a)** (i) Find the remainder when 24^{1947} is divided by 17. **(5+5)**

(ii) Show that 561 is a Carmichael number.

b) Solve the quadratic congruence $3x^2 - 4x + 7 \equiv 0 \, mod(13)$.

Q7 **a)** Prove that if p is an odd prime and $gcd(a,p) = 1$, then the congruence $x^2 \equiv a \, mod(p^n)$ for $n \geq 1$ has a solution if and only if $\left(\frac{a}{p}\right) = 1$. **(5+5)**

b) Prove that the value of any infinite continued fraction is an irrational number.

Q8 **a)** Let p be an odd prime and a be an integer such that $p \nmid a$. Let n denote the number of least positive residues of the integers $a, 2a, 3a, \cdots, [(p-1)/2]a$ that exceed $p/2$. Then prove that $(a/p) = (-1)^n$. **(5+5)**

b) Prove that every rational number can be represented by a finite simple continued fraction. Express $\frac{225}{157}$ as a finite simple continued fraction.