AW–1683

B.Sc. (Part–II) Semester–III Examination

MATHEMATICS

(Elementary Number Theory)

Paper—VI

Time : Three Hours] [Maximum Marks : 60

Note :— (1) Question No. **1** is compulsory and attempt it once only.

(2) Attempt **ONE** question from each unit.

1. Choose the correct alternative :—

(1) Two integers a and b that are not both zero are relatively prime whenever __________.

(a) $[a, b] = 1$ (b) $(a, b) = 1$

(c) $(a, b) = d, d > 1$ (d) None of these 1

(2) For $n \in N$, $(n, n + 1) =$ __________.

(a) 1 (b) n

(c) n + 1 (d) n(n + 1) 1

(3) A linear Diophantine equation $12x + 8y = 199$ has ________.

(a) unique solution (b) infinitely many solutions

(c) no solution (d) None of these 1

(4) Any two distinct Fermat numbers are __________.

(a) Composite (b) Relatively prime

(c) Prime numbers (d) None of these 1

(5) The non negative residue modulo 7 of 17 is __________.

(a) 0 (b) 1

(c) 2 (d) 3 1

(6) The inverse of 2 modulo 5 is __________.

(a) 3 (b) 2

(c) 5 (d) 1 1

(7) For any prime p, $\tau(p) =$ __________.

(a) 0 (b) 1

(c) 2 (d) None of these 1

(8) If n is divisible by a power of prime higher than one, then $\mu(n) =$ ________.

(a) 0 (b) 1

(c) n (d) n + 1 1

(9) The order of 3 modulo 5 is __________.

(a) 1 (b) 2

(c) 3 (d) 4 1

(1[illegible]) [illegible] of 7 is

(a) 3 (b) 4

(c) 5 (d) 6 1

UNIT—I

2. (a) Let $\frac{a}{b}$ and $\frac{c}{d}$ be fractions in lowest terms so that $(a, b) = (c, d) = 1$. Prove that if their sum is an integer, then $|b| = |d|$. 4

(b) Find the gcd of 275 and –200 and express it in the form $xa + yb$. 4

(c) If $(a, b) = d$, then show that $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$. 2

3. (p) Prove that a common multiple of any two non zero integers a and b is a multiple of the lcm $[a, b]$. 4

(q) If $(a, 4) = 2$ and $(b, 4) = 2$, then prove that $(a + b, 4) = 4$. 4

(r) Prove the $(a, a + 2) = 1$ or 2 for every integer a. 2

UNIT—II

4. (a) If P is a prime and $P \mid a_1a_2 \ldots\ldots a_n$, then prove that P divides at least one factor a_i of the product i.e. $P \mid a_i$ for some i, where $1 \le i \le n$. 5

(b) Find the gcd and lcm of $a = 18900$ and $b = 17160$ by writing each of the numbers a and b in prime factorization canonical form. 5

5. (p) Define Fermat number. Prove that the Fermat number F_5 is divisible by 641 and hence is composite. 1+4

(q) Find the solution of the linear Diaphantine equation $5x + 3y = 52$. 5

UNIT—III

6. (a) Prove that congruence modulo m is an equivalence relation. 6

(b) Solve the linear congruence

$$15x \equiv 10 \pmod{25}.$$ 4

7. (p) Solve the system of three congruences

$$x \equiv 1 \pmod 3,\ x \equiv 2 \pmod 5,\ x \equiv 3 \pmod 7.$$ 6

(q) If a, b, c and m are integers with $m > 0$ such that $a \equiv b \pmod m$, then prove that :

(i) $(a - c) \equiv (b - c) \pmod m$ 2

(ii) $ac \equiv bc \pmod m$. 2

UNIT—IV

8. (a) Define Euler ϕ-function. Prove that if P is a prime and k a positive integer, then

$$\phi(P^k) = P^{k-1}(P - 1).$$

Evaluate $\phi(3^4)$. 1+3+1

(b) If m is a positive integer and a is an integer with (a, m) = 1, then prove that

$a^{\phi(m)} \equiv 1 \pmod{m}$. 3

(c) Prove that, for any prime P,

$\sigma(P\,!) = (P + 1)\,\sigma((P - 1)!)$. 2

9. (p) State Mobius inversion formula.

Prove that if F is a multiplicative function and $F(n) = \sum_{d/n} f(d)$, then f is also multiplicative.

1+4

(q) Let $n = p_1^{a_1} p_2^{a_2} \ldots\ldots p_r^{a_r}$ be the prime factorization of the integer n > 1. If f is multiplicative function, prove that

$$\sum_{d/n} \mu(d) f(d) = (1 - f(p_1))(1 - f(p_2)).....(1 - f(p_r)).$$ 5

UNIT—V

10. (a) If P is an odd prime number, then prove that P^n has a primitive root for all positive integer n. 5

(b) Define the order of a modulo m. Given that a has order 3 modulo P, where P is an odd prime, show that a + 1 must have order 6 modulo P. 1+4

11. (p) Prove that the quadratic residues of odd prime P are congruent modulo P to the integers

$1^2, 2^2, \ldots\ldots, \left(\frac{P-1}{2}\right)^2$. 5

(q) Solve the quadratic congruence

$5x^2 - 6x + 2 \equiv 0 \pmod{13}$. 5