AU–82

B.Sc. Part—II (Semester—III) Examination
MATHEMATICS (New)
(Elementary Number Theory)
Paper—VI

Time : Three Hours] [Maximum Marks : 60

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

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

1. Choose the correct alternative :

(i) The product of any m consecutive integers is divisible by :

(a) $(m + 1)!$ (b) $(m - 1)!$

(c) $m!$ (d) $\frac{m}{2}!$

(ii) If c > 0 is common divisor of a and b, then $\left(\frac{a}{c}, \frac{b}{c}\right) =$

(a) $\frac{(a, b)}{c}$ (b) $\frac{[a, b]}{c}$

(c) $\frac{c}{(a, b)}$ (d) $\frac{c}{[a, b]}$

(iii) The conjecture "Every odd integer is the sum of at most three primes" is given by :

(a) Euler (b) Goldbach

(c) Eratothenes (d) None of these

(iv) If x > 0, y > 0 and x – y is even, then $x^2 - y^2$ is divisible by :

(a) 3 (b) 4

(c) 5 (d) 7

(v) If n > 2 is a positive integer, then :

$$1^3 + 2^3 + 3^3 + 4^3 + \ldots + (n - 1)^3 \equiv$$

(a) 0 (mod n) (b) 1 (mod n)

(c) 2 (mod n) (d) None of these

(vi) The set {0, 1, 2, 3} is complete system of residues modulo :

(a) 3 (b) 4

(c) 5 (d) 2

(vii) The function f is multiplicative, if :

(a) $f(mn) = f(m) | f(n)$ (b) $f(mn) = f(n) | f(m)$

(c) $f(mn) = f(m) f(n)$ (d) None of these

(viii) If n = 18, then the pair of $\tau(18)$ and $\sigma(18)$ is :

(a) (6, 39) (b) (6, 40)

(c) (7, 93) (d) (7, 92)

(ix) If $O_m(a) = n$, then $O_m(a^k) =$

(a) $\frac{m}{(m, k)}$ (b) $\frac{n}{(m, n)}$

(c) $\frac{n}{(n, k)}$ (d) None of these

(x) The quadratic residues of 7 are :

(a) (2, 3, 4) (b) (3, 5, 6)

(c) (1, 2, 4) (d) None of these 10

UNIT—I

2. (a) Find the gcd of 275 and 200 and express it in the form 275 x + 200 y. 4

(b) State and prove the division algorithm theorem. 1+3

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

3. (p) If a, b ∈ I, b ≠ 0 and a = bq + r 0 ≤ r < b, then show that (a, b) = (b, r). 4

(q) For positive integer a and b, prove that :

$(a, b)\,[a, b] = ab.$ 3

(r) Prove that there are no integers a, b, n > 1 such that $(a^n - b^n) \mid (a^n + b^n)$. 3

UNIT—II

4. (a) Prove that every positive integer greater than one has at least one prime divisor. 5

(b) Prove that the Fermat number F_5 is divisible by 641 and hence it is composite. 5

5. (p) Find the solution of the linear Diaphantine equation $10x + 6y = 110$. 5

(q) If P_n is the n^{th} prime number, then prove that :

$$P_n \le 2^{2^{n-1}}.$$ 5

UNIT—III

6. (a) Show that congruence is an equivalence relation. 5

(b) Find the solution of $140x \equiv 133 \pmod{301}$. 5

7. (p) If $a \equiv b \pmod{m}$, then prove that $a^n \equiv b^n \pmod{m}$, $\forall\ n \in N$. 5

(q) Solve the system of three congruences :

$$x \equiv 1 \pmod 4,\quad x \equiv 0 \pmod 3,\quad x \equiv 5 \pmod 7.$$ 5

UNIT—IV

8. (a) If m is a positive integer and a is an integer with $(a, m) = 1$, then prove that $a^{\phi(m)} \equiv 1 \pmod{m}$. 5

(b) If n is a positive integer, then prove that :

$$\sum_{d|n} \phi(d) = n.$$ 5

9. (p) Prove that the Möbius r-function is multiplicative. 4

(q) For $n > 2$, prove that $\phi(n)$ is an even integer. 3

(r) Find the value of $\tau(1800)$ and $\sigma(1800)$. 3

UNIT—V

10. (a) If $O_m(a) = n$, then prove that $a^k \equiv 1 \pmod{m}$ iff $n|k$, $\forall\ k \in N$. 3

(b) If $(a, m) = d > 1$, then prove that m has no primitive root a. 3

(c) If p is a prime and $d|p - 1$, then prove that the congruence $x^d - 1 \equiv 0 \pmod{p}$ has exactly d solutions. 4

11. (p) Find all the primitive roots of $p = 17$. 5

(q) Show that the congruence $x^2 \equiv a \pmod{p}$ has either no solutions or exactly two incongruent solutions modulo p. 5