AS–1401

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 (1 mark each) :

(i) If c > 0 is a common multiple of a and b, then $\left(\frac{c}{a}, \frac{c}{b}\right) =$ ______ .

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

(c) $c\left(\frac{1}{a}, \frac{1}{b}\right)$ (d) None of these

(ii) For $n \geq 1$, there are at least $(n + 1)$ primes ______ 2^{2^n}.

(a) Greater than (b) Less than

(c) Equal to (d) None of these

(iii) The set {0, 1, 2 ..., m – 1} is a complete system of residues modulo :

(a) m (b) m – 1

(c) m + 1 (d) None of these

(iv) The quadratic residues of 7 are :

(a) 1, 2, 3 (b) 3, 5, 6

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

(v) If P is a prime divisor of the Fermat number $F_n = 2^{2^n} + 1$, then $O_p(2)$ = ____.

(a) 2^n (b) 2^{n+1}

(c) 2^{2^n} (d) 2^{n-1}

(vi) The number of residues ________ the number of non residues.

(a) Equal (b) Not equal

(c) Greater than (d) Less than

(vii) If p is an odd prime, then $\left(-\frac{1}{p}\right) = -1$ if :

(a) $p \equiv 1 \pmod 4$ (b) $p \equiv -1 \pmod 4$

(c) $p \equiv 0 \pmod 4$ (d) None of these

(viii) If p is a prime, then $2^p + 3^p$ is :

(a) Perfect square (b) Not perfect square

(c) Prime (d) Positive integer

(ix) For a positive integer n, $(n - 1)! \equiv -1 \pmod n \Rightarrow$ n is :

(a) Prime (b) –ve integer

(c) Positive integer (d) Composite Number

(x) If $2^3 \equiv 1 \pmod 7$; $(2, 7) = 1$, then the order of 2 modulo 7 is :

(a) 1 (b) 2

(c) 3 (d) 7 10

UNIT—I

2. (a) Find positive integers a and b satisfying the equations (a, b) = 10 and [a, b] = 100 simultaneously, find all solutions. 3

(b) Find the values of x and y to satisfy the equation 423x + 198y = 9. 4

(c) If (a, b) = d, then show that $\left(\frac{a}{d}, \frac{b}{d}\right) = 1$. 3

3. (p) Prove that there are no integers a, b, n > 1 such that :

$$(a^n - b^n) \mid (a^n + b^n).$$ 3

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

(r) Using the Euclidean algorithm find the gcd d of the number 1109 and 4999 and then find integers x and y to satisfy d = 1109x + 4999y. 4

UNIT—II

4. (a) If $2^m + 1$ is prime, then show that m is a power of 2, for some non negative integer K. 3

(b) Find the solution of the linear Diaphantine equation 15x + 7y = 111. 4

(c) Show that :

$F_0F_1 \ldots F_{n-1} = F_{n-2}$, for all positive integers. 3

5. (p) Prove that every positive integer a > 1 can be written uniquely as a product of primes, apart from the order in which the factors occurs i.e. $a = p_1p_2 \ldots p_r$, all p_i being primes. 5

(q) If a prime p > 3, then show that 2p + 1 and 4p + 1 can not be prime simultaneously. 3

(r) If p is a prime and $p \mid ab$ then show that $p \mid a$ or $p \mid b$. 2

UNIT—III

6. (a) If $r_1, r_2 \ldots r_m$ is a complete system of residues modulo m and (a, m) = 1, a is a positive integer then prove that :

$a_{r_1} + b, a_{r_2} + b \ldots a_{r_m} + b$ is also complete system of residues modulo m. 5

(b) Solve the system of three congruences :

$x \equiv 1 \pmod 4$

$x \equiv 0 \pmod 3$

$x \equiv 5 \pmod 7$. 5

7. (p) Find the solutions of $15x \equiv 12 \pmod 9$. 4

(q) Show that 41 divide $2^{20} - 1$. 3

(r) Prove that $ca \equiv cb \pmod m$ iff $a \equiv b \left(\bmod \frac{m}{d}\right)$, where d = (c, m). 3

UNIT—IV

8. (a) Find the number of positive integers less or equal to 7200 that are prime to 3600. 3

(b) If $n = p_1^{a_1} p_2^{a_2} \dots p_m^{a_m}$ is the prime-power factorization of the positive integer n, then show that :

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\dots\left(1 - \frac{1}{p_m}\right). \quad 4$$

(c) If $n = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_m^{\alpha_m}$, then prove that :

$$\tau(n) = (\alpha_1 + 1)(\alpha_2 + 1) \dots (\alpha_m + 1). \quad 3$$

9. (p) Prove that the möbius μ-function is multiplicative. 5

(r) If m and n are two positive relatively prime integer, then show that $\phi(m\, n) = \phi(m)\, \phi(n)$. 5

UNIT—V

10. (a) If a and m are relatively prime positive integers and if a is a primitive root of m, then show that the integers a, a^2, ... $a^{\phi(m)}$ form a reduced residue set modulo m. 4

(b) Solve the quadratic congruence $x^2 + 7x + 10 \equiv 0 \pmod{11}$. 3

(c) If p is a prime number and $d|(p-1)$, then prove that the congruence $x^d - 1 \equiv 0 \pmod p$ has exactly d solutions. 3

11. (p) If p is an odd prime and a, b are integers with (a, p) = 1 = (b, p) then prove that :

(i) $a \equiv b \pmod p \Rightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$

(ii) $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$

(iii) $\left(\frac{a^2}{p}\right) = 1$. 5

(q) If p is a odd prime and a is a primitive root of p such that $a^{p-1} \not\equiv 1 \pmod{p^2}$, then show that for each positive integer $n \geq 2$

$$a^{p^{n-2}(p-1)} \not\equiv 1 \pmod{p^n}. \quad 5$$