2 0 1 9

(CBCS)

(6th Semester)

MATHEMATICS

TWELFTH (B) PAPER

(Elementary Number Theory)

Full Marks : 75

Time : 3 hours

(PART : A—OBJECTIVE)

(*Marks* : 25)

SECTION—A

(*Marks* : 10)

Answer **all** questions

Each question carries 1 mark

Put a Tick ☑ mark against the correct answer in the box provided :

1. If $(a, 4)$ 2 and $(b, 4)$ 2, then $(a \quad b, 4) =$

(a) 1 ☐

(b) 4 ☐

(c) 6 ☐

(d) 8 ☐

2. The square of any integer of the form $5k \quad 1$ is of the form

(a) $5k \quad 1$ ☐

(b) $5k$ ☐

(c) $5k \quad 1$ ☐

(d) $5(k \quad 1)$ ☐

3. Choose the odd one out.

(a) $a \quad b \pmod m$ ☐

(b) $b \quad a \pmod m$ ☐

(c) $a \quad b \quad 0 \pmod m$ ☐

(d) $a \quad m \pmod b$ ☐

4. The complete residue system modulo 17 composed entirely of multiples of 3 is

(a) {18, 36, 21, 39, 24, 42, 27, 45, 30, 48, 33} ☐

(b) {0, 3, 9, 12, 15, 18, 21, 24, 27, 30, 33, 36} ☐

(c) {0, 18, 36, 3, 21, 39, 6, 24, 42, 9, 27, 45, 12, 30, 48, 15, 33} ☐

(d) {18, 36, 3, 21, 39, 6, 24, 42, 9, 27, 45, 12, 30, 48, 15, 33, 51} ☐

5. Let p be a prime, then $x^2 \quad 1 \pmod p$ has a solution if and only if

(a) $p \quad 2$ or $p \quad 2 \pmod 4$ ☐

(b) $p \quad 4$ or $p \quad 4 \pmod 4$ ☐

(c) $p \quad 4$ or $p \quad 2 \pmod 4$ ☐

(d) $p \quad 2$ or $p \quad 1 \pmod 4$ ☐

6. If p is a prime such that p does not divide a, where a is an integer, then

(a) $a^{p \quad 1} \quad 1 \pmod p$ ☐

(b) $a^{p} \quad 1 \pmod p$ ☐

(c) $a^{p \quad 1} \quad a \pmod p$ ☐

(d) $a^{p} \quad p \pmod a$ ☐

7. The congruence $f(x)$ 0(mod p) of degree n has at most

(a) n 1 solutions ☐

(b) n solutions ☐

(c) n 1 solutions ☐

(d) n^2 solutions ☐

8. If p denotes an odd prime and (a, p) 1, then the Legendre symbol $\frac{a}{p}$ is

(a) 1 if a is a quadratic non-residue modulo p and –1 if a is a quadratic residue ☐

(b) 0 if a is a quadratic residue and 1 if a is a quadratic non-residue modulo p ☐

(c) 1 if a is a quadratic residue and –1 if a is a quadratic non-residue modulo p ☐

(d) 0 if a is a quadratic non-residue modulo p and 1 if a is a quadratic residue ☐

9. If (n) is odd, then n is of the form

(a) k^2 or k^3 ☐

(b) k^2 or $2k^2$ ☐

(c) k or $2k$ ☐

(d) k or $2k^2$ ☐

10. An arithmetic function $f(n)$ not identically zero is said to be multiplicative if for every pair of positive integers m and n

(a) $f(mn)$ $f(m)f(n)$ and (m, n) 1 ☐

(b) $f(mn)$ $f(nm)$ and (m, n) 1 ☐

(c) $f(mn)$ $f(m)f(n)$ and (m, n) 1 ☐

(d) $f(mn)$ $f(m)f(n)$ and (m, n) 1 ☐

SECTION—B

(*Marks* : 15)

Each question carries 3 marks

1. *(a)* Using Euclidean algorithm, find the GCD of 7468 and 2464.

OR

(b) Prove that if (a, b) 1 and (b, c) 1, then (ac, b) 1.

2. *(a)* Prove that the number of primes is infinite.

OR

(b) If a b (mod m), a b (mod n) and (m, n) 1, then show that a b (mod mn).

3. *(a)* Show that (mn) n (m) if every prime that divides n also divides m.

OR

(b) Find the number of positive integers 3600 that are prime to 3600.

4. *(a)* Solve $295x$ 5 (mod 11).

OR

(b) If q $4p$ 1, where p is an odd prime, then show that 2 is a primitive root of q.

5. *(a)* Find the value of (2520).

OR

(b) Solve $5x$ $3y$ 52.

(PART : B—DESCRIPTIVE)

(*Marks* : 50)

The figures in the margin indicate full marks for the questions

Answer **five** questions, taking **one** from each Unit

UNIT—I

1. *(a)* If g is the greatest common divisor of the integers a and b, then prove that there exist integers x_0 and y_0 such that g (a, b) ax_0 by_0. Using Euclidean algorithm, find the least values of x_0 and y_0 such that $71x_0$ $50y_0$ 1. 5+2=7

(b) Show that 4 does not divide $n^2 \quad 4$, where n is odd integer. 3

2. (a) State and prove the fundamental theorem of arithmetic. 1+6=7

(b) Show that if p is prime and p / ab, then p / a or p / b, where a and b are any two integers. 3

UNIT—II

3. (a) Prove that there are arbitrary large gaps in the series of primes, that is, given any positive integer k, there exists k consecutive composite integers. 5

(b) Prove that $ax \quad ay \pmod{m}$ if and only if $x \quad y \bmod \frac{m}{(a, m)}$. 5

4. (a) If p is a prime, prove that $(a \quad b)^m \quad a^m \quad b^m \pmod{m}$. 5

(b) Find the smallest value of $|36^m \quad 5^n|$, where m and n are positive integers. 5

UNIT—III

5. (a) If p is a prime, then prove that $(p \quad 1)! \quad 1 \pmod{p}$. 5

(b) If $n \quad 1$, prove that $(n) \quad n \quad {}_{p/n} \; 1 \quad \frac{1}{p}$, where ${}_{p/n}$ is the product over all primes that divide n. 5

6. (a) If $(a, m) \quad 1$, then prove that $a^{(m)} \quad 1 \pmod{m}$, where is Euler's -function. 5

(b) If a positive integer n has k distinct odd prime factors, prove that $2^k | \; (n)$. 5

UNIT—IV

7. (a) Using Chinese remainder theorem, solve

$$x \quad 5 \pmod{18}$$
$$x \quad 1 \pmod{24}$$
$$x \quad 17 \pmod{33}$$

4

(b) If p and q are distinct odd primes, then prove that

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$$

where $\left(\frac{p}{q}\right)$ is a Legendre symbol. 6

8. (a) State and prove Gauss' lemma. 1+5=6

(b) If p is a prime and $(a, p) = 1$, then prove that $x^n \equiv a \pmod{p}$ has $(n, p-1)$ solutions or no solution according as $a^{\frac{p-1}{(n, p-1)}} \equiv 1 \pmod{p}$ or $a^{\frac{p-1}{(n, p-1)}} \not\equiv 1 \pmod{p}$. 4

UNIT—V

9. Find all the Pythagorean triples (x, y, z) in $x^2 + y^2 = z^2$ whose terms form (a) an arithmetic progression and (b) a geometric progression. 5+5=10

10. (a) State and prove Möbius Inversion theorem. 1+5=6

(b) Prove that $\sigma_k(n) = n^k \sigma_{-k}(n)$. 4

★ ★ ★