63/1 (SEM–5) DSE1/MATHE5016

2023

MATHEMATICS

Paper : MATHE5016

(Number Theory)

Full Marks : 80

Pass Marks : 32

Time : Three hours

The figures in the margin indicate full marks for the questions.

1. Choose the correct option from the following : ***(any six)*** 1×6=6

   (a) If $\pi(x)$ denotes prime counting function, then $\pi(10)$ is

   (i) 2

   (ii) 3

   (iii) 4

   (iv) 10

(b) If $a \equiv b(mod m)$ and $c(\neq 0)$ is any integer, then which of the following is not true?

(i) $a+c \equiv (b+c)(mod m)$

(ii) $a-c \equiv (b-c)(mod m)$

(iii) $ab \equiv bc\,(mod m)$

(iv) $\frac{a}{c} = \frac{b}{c}(mod m)$

(c) Let 'a' and 'b' be two positive integers. Then $gcd(a,b).\ lcm[a,b]$ is

(i) ab

(ii) a/b

(iii) b/a

(iv) $a+b$

(d) The congruence $ax \equiv 1(mod m)$ has unique solution, if

(i) $(a, m) = 1$

(ii) $(a, m) > 1$

(iii) $(a, m) < 1$

(iv) $(a, m) \neq 1$

(e) The value of $\left[-\frac{3}{2}\right]$ is

(i) -2

(ii) -1

(iii) 2

(iv) 1

where $[x]$ denotes greatest integer less than or equal to x.

(f) If n is prime, then $\phi(n)$ is

(i) n

(ii) $n-1$

(iii) $n+1$

(iv) $\lfloor n$

(g) The Mobius function $\mu(x)$ is

(i) Multiplicative

(ii) Completely multiplicative

(iii) Both (i) and (ii)

(iv) Neither (i) nor (ii)

(h) Which of the following is not Pythagorean triple ?

(i) $(3, 4, 5)$

(ii) $(2, 3, 4)$

(iii) $(4, 5, 6)$

(iv) $(1, 2, 3)$

(i) If $gcd(a, b) = d$, then a Diophantine equation $ax + by = c$ is solvable, iff

(i) $d \mid c$

(ii) $d \nmid c$

(iii) $d = c$

(iv) $d \neq c$

(j) 'a' is called a primitive root of m if, $0\,(a(mod m))$ is

(i) $\mu(m)$

(ii) $\tau(m)$

(iii) $\varphi(m)$

(iv) $\sigma(m)$

2. Answer the following questions : ***(any five)*** 2×5=10

(a) Find the integral solution of the linear Diophantine equation

$$8x - 10y = 42$$

(b) Find the remainder when 5^{48} is divided by 24.

(c) Evaluate the order of
$5^6 \pmod{12}$

(d) Prove that if x and y are odd, then $x^2 + y^2$ is even but not divisible by 4.

(e) Find the number of positive divisors and the sum of positive divisors of 36.

(f) Show that $\sum_{d|10} \mu(d) = 0$

(g) Define encryption and decryption in cryptosystem.

3. Answer ***any six*** questions : 5×6=30

(a) Let $a, b \in Z$, not both of which are zero and $d = gcd(a, b)$. Then prove that there exist integers x and y such that $d = ax + by$.

(b) Define Euler's phi-function. Show that
(i) $\phi(3n) = 2\phi(n)$, iff $3 \nmid n$
(ii) $\phi(3n) = 3\phi(n)$, iff $3 | n$
1+(2+2)=5

(c) Solve the linear congruence
$6x \equiv 15 \pmod{21}$

(d) If 'a' is a primitive root of m, then show that a^k is also a primitive root of m iff $(k, \phi(m)) = 1$.

(e) If n is a square free integer, prove that $\tau(n) = 2^K$, where K is the number of prime divisor of n.

(f) Show that there are no positive integers n satisfying $\sigma(n) = 10$.

(g) If f is a multiplicative function and F is defined by
$$F(n) = \sum_{d|n} f(d)$$
prove that F is also multiplicative. Hence show that the functions τ and σ are multiplicative. 3+2=5

(h) Prove that the necessary and sufficient condition that 'a' is a quadratic residue of m when m is odd prime, $(a, m) = 1$ is $a^{\frac{m-1}{2}} \equiv 1 \pmod{m}$.

(i) Solve the quadratic congruence

$$x^2 \equiv 7 (mod 3^3).$$

(j) Prove that the Diophantine equation $x^2 + y^2 = z^2$ has a primitive solution (a, b, c), if one of 'a' or 'b' is even and the other is odd.

4. Answer ***any two*** of the following questions : 10×2=20

(a) Let 'a' be any integer, p be prime and let p do not divide 'a'. Then prove that

$$a^{p-1} \equiv 1 (mod\, p)$$

Is the converse true ? Justify your answer. 6+4=10

(b) (i) Define $\sigma(n)$.

If $n = p_1^{k_1} p_2^{k_2} p_3^{k_3} \cdots p_r^{k_r}$ is the prime factorisation of $n > 1$, then prove that

$$\sigma(n) = \prod_{i=1}^{r} \frac{p_i^{k_i+1} - 1}{p_i - 1}$$ 5

(ii) If $f(n)$ be a function of n, then prove that

$$\sum_{d|n} f(d) = \sum_{d|n} f\left(\frac{n}{d}\right),$$

where n is a +ve integer ≥ 1. 5

(c) (i) If $a \equiv b (mod m)$, then show that $a^k \equiv b^k (mod m)$, for any positive integer $k > 1$. Is the converse true ? Justify your answer. 3+2=5

(ii) Prove that any primitive solution of $x^2 + y^2 = z^2$ is of the form $(2ab, a^2 - b^2, a^2 + b^2)$ for some integers 'a' and 'b' such that $a > b > 0$, $(a, b) = 1$ and $a + b \equiv 1 (mod 2)$. 5

(d) (i) If $a, b \in Z$, then show that a positive integer 'p' is a prime if and only if $p | ab \Rightarrow p | a$ or $p | b$. 5

(ii) Prove that if $f(n)$ is multiplicative then

$$\sum_{d|n} \mu(d) f(d) = \prod_{p|n} (1 - f(p))$$ 5

5. Answer ***any one*** part : 14×1=14

(a) State and prove Chinese remainder theorem. Using the theorem, solve the system of congruences

$x \equiv 2 \pmod 3$

$x \equiv 3 \pmod 5$

$x \equiv 2 \pmod 2$ 2+7+5=14

(b) (i) Explain with example how the RSA cryptosystem works. 8

(ii) Find the integers n, E and X such that $X^E \equiv X \pmod n$

Is this a potential problem in the RSA cryptosystem ? 6

(c) (i) If p is an odd prime, then prove that there is at least one primitive root p such that

$a^{p-1} \not\equiv 1 \pmod{p^2}$ 5

(ii) If p and q be the distinct primes with

$a^p \equiv a \pmod q$ and

$a^q \equiv a \pmod p$, then

prove that $a^{pq} \equiv a \pmod{pq}$ 5

(iii) Define quadratic residue and quadratic non-residue.
For the quadratic congruence $x^2 \equiv a \pmod 7$, determine the values of 'a' for which $a R 7$ and $a \not R 7$, where $a R 7$ means 'a' is a quadratic residue of 7 and $a \not R 7$ means 'a' is non-quadratic residue of 7. 4