Total number of printed pages = 9

63/1(SEM-5) DSE1 MATHE5016

2024

MATHEMATICS

Paper : MATHE5016

(Number Theory)

Full Marks : 80

Pass Marks : 32

Time : 3 hours

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

1. Choose the correct answer ***(any six)*** : $1\times6=6$

(a) If a and b are non-zero integers with $a \mid b$, then gcd(a,b) equals

(i) $|a|$ *(ii)* b

(iii) ab *(iv)* a

(b) Which of the following Diophantine equation can not be solved?

(i) $6x+51y=22$ *(ii)* $33x+14y=115$

(iii) $14x+35y=93$ *(iv)* $11x+13y=21$

(c) The unit digit of 3^{100} is

(i) 1 *(ii)* 2

(iii) -1 *(iv)* -2

(d) For $a, m \in Z$, $a\sigma^{\phi(m)} \equiv 1 (\mathrm{mod}\, m)$, if

(i) $(a, m) \neq 1$ *(ii)* $(a,m)=1$

(iii) $m \mid a$ *(iv)* $a \mid m$

(e) If $\sigma(n)$ denotes the sum of positive divisors, then $\sigma(12)$ is

(i) 28 *(ii)* 25

(iii) 16 *(iv)* 10

(f) If $a \equiv b$ mod(n), where $a,b,n \in Z$ and $n>0$. If $\gcd(a,n)=d$, then gcd (b,n) is

(i) 1 *(ii)* nd

(iii) d *(iv)* na

(g) If a is a whole number and P is a prime number, then according to Fermat's Little's theorem __.

(i) $2^{P-1}-2$ is divisible by P

(ii) $2^{P}-1$ is divisible by P

(iii) $2^{P}-2$ is not divisible by P

(iv) $2^{P}-2$ is divisible by P

Contd.

(h) If $\phi(n)$ denotes Euler phi-function, then $\phi(15)$ is ___.

(i) 5 (ii) 8

(iii) 10 (iv) 6

(i) Necessary condition to apply the Chinese remainder theorem is moduls of congruence should be

(i) Individually prime

(ii) Relatively prime

(iii) No relatively prime

(iv) No restriction on modulo

(j) If P is a prime, then

(i) $(P-1)! \equiv 1 \bmod P$

(ii) $(P-1)! \equiv -1 \bmod P$

(iii) $(P-1)! \equiv P \bmod P$

(iv) $(P-1)! \equiv -P \bmod P$

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

(a) If P is a prime and $P \mid ab$, then prove that either $P \mid a$ or $P \mid b$.

(b) Prove that the product of two or more integers of the form $4n+1$ is of the same form.

(c) Show that 41 divides $2^{20}-1$.

(d) If $ca \equiv cb \pmod{n}$, then prove that

$a \equiv b \pmod{n \mid b}$, where d= gcd(c,n).

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

(f) For a positive integer γ, prove that the product of any γ consecutive positive integers is divisible by $\gamma!$

(g) If $F_n = 2^{2n}+1$, $n>1$ is a prime, then show that 2 is not a primitive root of F_n.

3. Answer the following questions ***(any six)***: 5×6=30

(a) Find all the possible solutions in positive integers of the Diophantive equation

$$172x + 20y = 1000$$

(b) Prove that for arbitrary integers a and b, $a \equiv b \pmod{n}$ if and only if a and b

leave the same non-negative remainder when divided by n.

(c) Find the remainder when $2^{73}+24^3$ is divided by 11.

(d) Prove that there are infinitely many primes.

(e) Prove that the linear congruence $ax \equiv b \pmod{n}$ has a sulution if and only if d | b, where $d=\gcd(a,n)$.

(f) State and prove wilson's theorem.

(g) Solve the linear congruence $39x \equiv 65 \pmod{52}$

(h) Prove that the functions τ and σ are both multiplicative functions.

(i) Let $\gcd(a,n)=1$ and let $a_1, a_2, \ldots a_{\cdot\cdot}$ be the positive integers less than n and relatively prime to n. if a is a primitive root of n, then prove that $a, a^2, \ldots, a^{\phi(n)}$ are congruent modulo n to $a_1, a_2, \ldots, a_{\phi(n)}$, in some order.

(j) If P be an odd prime and $\gcd(a,p)=1$ then prove that the congruence

$x^2 \equiv a \pmod{Pn}$, $n>1$

has a solution if and only if $\left(\frac{a}{p}\right)=1$.

4. Answer the following question ***(any two)***: 10×2=20

(a) (i) Show that the system of linear

Congruences $ax+by \equiv \gamma \pmod{n}$

$cx+dy \equiv s \pmod{n}$

has a unique modulo n whenever

$\gcd(ad-bc,n)=1$

(ii) Find all the integers that gives remainders 1,2,3 when divided by 3,4,5 respectively. 4+6=10

(b) (i) Show that the quadratic congruence $x^2+1 \equiv 0 \pmod{P}$ where P is an odd prime, has a solution if and only if $P \equiv 1 \pmod{4}$.

(ii) State and prove Mobius inversion formula. 5+5=10

(c) (i) Let f and F be number-theoretic functions such that $F(n)=\sum_{d/n} f(d)$, then for any positive integer N, prove that $\sum_{n=1}^{N} F(n)=\sum_{n=1}^{N} f(n)\left(\frac{N}{K}\right)$.

*(ii)*Define Euler's phi-function.

If the integer $n>1$ has the prime factorization $n = P_1^{K1}P_2^{K2}...P_\gamma^{K\gamma}$, then

$$\phi(n) = n \prod_{i=1}^{\gamma} (1-\tfrac{1}{P_i}).$$ 5+5=10

(d) *(i)* If $n>1$ and gcd$(a,n)=1$, then prove that $a^{\phi(n)} \equiv 1 \pmod{n}$.

*(ii)*If gcd $(m,n)=1$, where $m>2$ and $n>2$, then prove that the integer mn has no primitive roots. 5+5=10

Answer the following question ***(any one)***: 14×1=14

(a) *(i)* If P is a prime, then prove that $a^P \equiv a \pmod{p}$ for any integer a.

*(ii)*If n and γ are positive integers with $1<\gamma<n$, then prove that the binomial coefficient

$$\binom{n}{\gamma} = \frac{n!}{\gamma!(n-\gamma)!}$$ is also an integer.

(iii) Define Mobius V function. Show that V is a multiplicative function. 5+5+4=14

(b) *(i)* Define primitive pythagorean triple with example. 2+4=6

If x,y,z is a primitive Pythagorean triple, then prove that one of the integers x or y is even, while the other is odd.

*(ii)*Prove that the Diophantine equation $x^4+y^4=z^2$ has no solution in positive integers x,y,z. 8

(c) *(i)* Explain with example how the public key cryptography works.

*(ii)*If $n = P_1^{K2}P_2^{K2}....P_\gamma^{K\gamma}$ is the prime factorization of $n>1$, then prove that the positive divisors of n are precisely those integers d of the form

$$d = P_1^{a2}P_2^{a2}....P_\gamma^{a\gamma}$$

Where $0 \le a_i \le K_i$ $(i=1,2,....,\gamma)$ 8+6=14