

Department of Mathematics
Pattamundai College, Pattamundai

5th Semester
Number Theory

DSE - II

Sec - A Unit - I

1. If a/b and b/c imply a/c . (T/F)
2. If a is any positive integer, then $1+a+a^2$ is not a square number prove it.
3. Find the greatest common divisor of 525 and 231.
4. Determine the linear diophantine equation $12x+18y=30$ is solvable.
5. The linear diophantine equation $a_1x_1+a_2x_2+\dots+\dots+a_nx_n = C$ is solvable if and only if $\gcd(a_1, a_2, a_3, \dots, a_n)/c$.
When it is solvable it has _____ solutions.
6. Determine if the linear diophantine equations.
 $6x+8y + 12z = 10$ and $6x+12y+15z=10$ are solvable.
7. What is the meaning of twin primes and give an example of twin primes.
8. If P is a prime then $p+2$ is a prime. (T/F)
9. If P is a prime then p^2+1 is a prime (T/F)
10. There are an infinite number of composite numbers (T/F)
11. There are primes of the form $(n!+1)$. (T/F)
12. Show that every prime need not odd.

UNIT - 2

13. Show that $a \equiv b \pmod{m}$ is symmetric.
14. The congruence relation is an equivalence relation . (T/F)
15. If $a \equiv b \pmod{m}$ then $a^2 \equiv b^2 \pmod{m}$ (T/F)
16. If $a \equiv b \pmod{m}$ then find the difference between the least residue and minimal residue.
17. Find the remainder when 5^{48} is divided by 24.
18. Show that $8x \equiv 10 \pmod{6}$ has two incongruent solutions modulo 6.
19. If p is a prime and $(a,p) = 1$ then $a^{p-1} - 1$ is divisible by _____
20. The integer n if and only if $(n-1)! + 1 \equiv 0 \pmod{n}$ Then n is _____

21. The linear system $x \equiv a \pmod{m}$ and $x \equiv b \pmod{n}$ is solvable if and only if $f(m,n) \mid (a-b)$. when it has unique solution ?
22. If $a \equiv b \pmod{m_1}$, $a \equiv b \pmod{m_2}$,..... $a \equiv b \pmod{m_k}$ then $a \equiv b \pmod{[m_1, m_2, m_3, \dots, m_k]}$. (T/F)
23. If $ac \equiv bc \pmod{m}$ and $\gcd(c,m) = d$ then $a \equiv b \pmod{m}$ then find the value of d ?
24. Find the positive integers n for which $\sum_{k=1}^n k!$ is a square.

UNIT - 3

25. A number theoretic function f is multiplicative if $f(mn) = f(m).f(n)$. where m and n are relatively prime.
26. Show that the constant function $f(n) = 1$ is multiplicative.
27. Compute $\phi(15625)$
28. Prove each, when n and e are positive integers $\phi(n^2) = n\phi(n)$
29. Evaluate $\sigma(12)$ and $\sigma(28)$
30. Compute $z(36)$ and $z(49)$
31. Define the mobius function μ
32. Determine if $\mu(mn) = \mu(m) \cdot \mu(n)$ where $m = 15$ and $n = 28$.
33. If $n = 81$ then find $\sum_{d/n} \mu(d)$
34. Verify the formula $\phi(n) = n \sum_{d/n} \frac{\mu(d)}{d}$, where $n = 14$.
35. The sum of $\phi(m)$, positive integers less than m and relatively prime to m is $\frac{m}{2} \phi(m)$ (T/F)
36. If n is an odd integer, then $\phi(2n) = \underline{\hspace{2cm}}$

UNIT - 4

37. Find the order of 2 in modulo 7.
38. Order and primitive roots are both connected with modulo. (T/F)
39. If the order of a and b modulo m are λ and μ respectively and $\gcd(\lambda, \mu) = 1$ then the order of ab modulo m is _____.
40. The necessary and sufficient condition that 'a' is a primitive root of m is that $a, a^2, a^3, \dots, a^{\phi(m)}$ form the reduced residue system of m . (T/F)
41. The even number of a primitive root of an odd prime p is a quadratic residue of p justify your answer.
42. Show that if p is an odd prime then p^2 has a primitive root.
43. If m has a primitive root, then it has a total of $\phi(\phi(m))$ incongruent primitive roots. (T/F)
44. If p is an odd prime and the order of a modulo p is d ($< p-1$), then $a^\lambda, 1 \leq \lambda \leq d$ are all not its primitive roots(T/F)

45. The quadratic congruence $ax^2+bx+c \equiv 0 \pmod{p}$ can be reduced to the form $y^2 = d \pmod{p}$ where $y = 2ak+b$ and $d = b^2 - 4ac$. (T/F)
46. When one of a, b is a quadratic residue of p and the other is a non residue then $a.b$ is _____ ?
47. When $a \equiv b \pmod{p}$, then $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ (T/F)
48. If p is an odd prime and a and p are any integers coprime to p then $\left(\frac{ab^2}{p}\right) =$ _____ ?
49. Find the value of $\left(\frac{168}{11}\right)$
50. Find n of Gauss lemma for $\left(\frac{5}{19}\right)$

SEC - B , Unti - 1

1. If $c = ax + by$ and d/a but d/c , then prove that d/b .
2. Show that one of every three consecutive integers is divisible by 3.
3. The integers a and b are relative prime if and only if there exists integers x and y such that $ax+by = 1$.
4. Find the g.c.d of 28 and 49. Express it as linear combination of these numbers.
5. If $k > 0$ is a common multiple of a and b then $\left(\frac{k}{a}, \frac{k}{b}\right) = \frac{k}{[a,b]}$
6. If p is a prime and $p|b$ then $p|a$ or $p|b$.
7. Find the number of trailing zeros in $234!$
8. Solve, the linear diophantine equation $12x+6y=18$
9. Find the solution, if, exist, of the linear diophantine equation is solvable
 $2x + 3y + 4z = 5$.
10. If p is the r^{th} prime number then $p_r \leq 2^{2^r} - 1$
11. If $(n>2)$ terms of an A.P, $P, p+d, p+2d, \dots, p+(n-1)d$ are all prime numbers then common difference d is divisible by every prime $q>n$.
12. Show that, If $n>3$, then $P_{n+1}^2 < P_1.P_2.P_3 \dots P_n$.

UNIT - 2

13. $a \equiv b \pmod{m}$ if and only if $a = b+km$ for some integer k .
14. If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$ then $a \equiv c \pmod{m}$.
15. $a \equiv b \pmod{m}$ if and only if a and b leave the same remainder when divided by m .
16. Prove that no prime of the form $(4n+3)$ can be expressed as the sum of two squares.
17. If $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then prove that $a - c \equiv b - d \pmod{m}$.
18. Prove that no integer of the form $8n+7$ can be expressed as a sum of three squares.
19. If $a \equiv b \pmod{m}$ then prove that $a^n \equiv b^n \pmod{m}$ for any positive integer n .
20. If $a \equiv b \pmod{m}$ and c is any integer then prove that $ac \equiv bc \pmod{m}$

21. Compute the remainder when 3^{247} is divided by 25.
22. Solve the congruence $12x \equiv 48 \pmod{18}$
23. If p and q are distinct primes such that $a^p \equiv a \pmod{p}$ and $a^q \equiv a \pmod{q}$. Then prove that $a^{pq} \equiv a \pmod{pq}$
24. The odd prime factor of $(a^{2^n} + 1)$, ($a > 1$) is of the form $2^{n+1}t + 1$. Prove it.

UNIT - 3

25. A positive integer P is a prime if and only if $\phi(p) = p - 1$.
26. Let f be a multiplicative function and n a positive integer with canonical decomposition $n = p_1^{e_1} \cdot p_2^{e_2} \cdot p_3^{e_3} \dots p_k^{e_k}$ then $f(n) = f(p_1^{e_1}) \cdot f(p_2^{e_2}) \dots f(p_k^{e_k})$
27. Let P be a prime and e any positive integer.
Then $\phi(p^e) = p^e - p^{e-1}$.
28. Let $n = p_1^{e_1} \cdot p_2^{e_2} \dots p_k^{e_k}$ be the canonical decomposition of a positive integer 'n'.

$$\text{Then } \phi(n) = n \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \dots \left(1 - \frac{1}{p_k}\right)$$

29. If $n \geq 3$ then prove that $\phi(n)$ is even.
30. Let n be a positive integer - Then $\sum_{d|n} \phi(d) = n$
31. Determine if $F(mn) = F(m) \cdot F(n)$ where $m = 4$ and $n = 7$
32. Show that tau and sigma functions are multiplicative.
33. Determine if $\mu(mn) = \mu(m) \cdot \mu(n)$, where $m = 15$ and $n = 28$.
34. Show that function μ is multiplicative.
35. If $\phi(n) = n \sum_{d|n} \frac{\mu(d)}{d}$, verify the formula for $n = 12$.

36. Let n be a positive integer. Then prove that $\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{otherwise} \end{cases}$

UNIT - 4

37. If the order of 'a' modulo n is λ , then prove that $a^r \equiv a^s \pmod{n}$ if and only if $r \equiv s \pmod{\lambda}$
38. If the order of a modulo m is λ , then order of a^k is $\frac{\lambda}{\gcd(\lambda, k)}$
39. If P is prime and $d|(p-1)$, then the congruence $x^d - 1 \equiv 0 \pmod{p}$ has exactly d solutions.
40. Find the incongruent solutions of the congruence $x^3 - 1 \equiv 0 \pmod{3}$

41. If m has a primitive root then prove that $\phi(\phi(m))$ is also primitive roots.
42. If P is a prime a primitive root, then it has $\phi(p-1)$ primitive roots.
43. If $(a,m) = 1$, then a is a primitive root of m if and only if $a^{\frac{\phi(m)}{p}} \not\equiv 1 \pmod{m}$

for every prime divisor p of $\phi(m)$.

44. If $m,n > 2$ and $(m,n)=1$ when there exist no primitive roots mod (mn)
45. If the congruence $x^2 \equiv a \pmod{p}$ is solvable, then it has exactly two solutions.
46. Solve the congruence, $3x^2+5x+9 \equiv 0 \pmod{11}$
47. If $(a,p) = 1$, then either

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p} \text{ or } a^{\frac{p-1}{2}} \equiv -1 \pmod{p}$$

48. If P is an odd prime and a,b any integers coprime to p , then the legendre's symbol has the following propertie.

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

49. If P is an odd prime, then $\sum_{n=1}^{p-1} \left(\frac{n}{p}\right) = 0$

50. There are infinitely many primes of the form 4^{m+1} , where m is even integer.

SEC - C - UNIT - I

1. If g is the greatest common divisor of a and b , then there exists integers x any y such that $g=(a,b)= ax+by$
2. Every positive integer $n \geq 2$ is either a prime or can be expressed as a product of primes. The factorization into primes is unique except for the order of the factors.
3. The linear diophantine equation $ax+by = c$ is solvable if and only if $d|c$, where $d = \gcd(a,b)$. If x_0 and y_0 is a particular solution of the linear diophantine equation, then all its solutions are given by

$$x = x_0 + \left(\frac{b}{d}\right)t, y = y_0 - \left(\frac{a}{d}\right)t, \text{ where } t \text{ is an arbitrary integer.}$$

4. If a cock is worth five coins, a hen three coins and three chicks together one coin, how many cocks, hens and chicks, totaling 100, can be bought for 100 coins ?
5. Prove that there are at least $3\lfloor n/2 \rfloor$ primes in the range n through $n!$ where $n \geq 4$.

UNIT - 2

6. Find the remainder when $(n^2+n+41)^2$ is divided by 12.
7. The linear congruence $ax \equiv b \pmod{m}$ is solvable if and only if $d|b$, where $d = \gcd(a,m)$. If $d|b$ then prove that it has d incongruent solutions.
8. State and prove chinese remainder theorem.
9. Solve the system of linear congruences
 $x \equiv 5 \pmod{11}, x \equiv 14 \pmod{29}, x \equiv 15 \pmod{31}$
10. State and prove wilsons theorem.

UNIT - 3

11. Prove that the function ϕ is multiplicative.
12. If f is a multiplicative function, then $F(n) = \sum_{d|n} f(d)$ is also multiplicative.
13. Let n be a positive integer with cononical decomposition $n = P_1^{e_1} P_2^{e_2} P_3^{e_3} \dots P_k^{e_k}$. Then $\tau(n) = (e_1+1)(e_2+1)(e_3+1)\dots(e_k+1)$ and

$$\sigma(n) = \left(\frac{P_1^{e_1+1} - 1}{P_1 - 1} \right) \left(\frac{P_2^{e_2+1} - 1}{P_2 - 1} \right) \left(\frac{P_3^{e_3+1} - 1}{P_3 - 1} \right) \dots \left(\frac{P_k^{e_k+1} - 1}{P_k - 1} \right)$$

14. Let f be a number - theoretic function and let $f(n) = \sum_{d|n} f(d)$. Then prove that $f(n) = \sum_{d|n} \mu(d).F(n/d)$
15. Let F and f be number theoretic functions such that $f(n) = \sum_{d|n} \mu(d).F(n/d)$. Then prove that $F(n) = \sum_{d|n} f(d)$

UNIT - 4

16. If P is prime and $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + x_0$
 $a_n \not\equiv 0 \pmod{p}$ is a polynomial of degree $n \geq 1$ with integral coefficient the $f(x) \equiv 0 \pmod{p}$ has at least n is congruent solutions mod p .
17. If P is a prime and $d|p-1$, then prove that there are exactly $\phi(d)$ in congruent integers having d modulo p .
18. Find the primitive roots of 15 and 10.
19. Solve the linear congruence : $7x \equiv 2 \pmod{a}$
20. Prove that $n = \sum_{k=1}^{\frac{1}{2}(p-1)} \left[\frac{ka}{p} \right] + \frac{p^2-1}{8} (a-1) \pmod{2}$

--0--