THEORY OF NUMBERS

K1 QUESTIONS:

UNIT 1:

1. The linear combination of gcd (252, 198) = 18 is _____.
   a) 252*4 – 198*5
   b) 252*5 – 198*4
   c) 252*5 – 198*2
   d) 252*4 – 198*4
2. The inverse of 4 modulo 7 is
   a) -1
   b) 0
   c) -3
   d) -4
3. The linear combination of gcd(117, 213) = 3 can be written as
   a) 11*213 + (-20)*117
   b) 10*213 + (-20)*117
   c) 11*117 + (-20)*213
   d) 20*213 + (-25)*117
4. The inverse of 13 modulo 26 is
   a) 12
   b) 14
   c) 17
   d) 20
5. The solution of the linear congruence 4x = 5(mod 9) is
   a) 6(mod 9)
   b) 8(mod 9)
   c) 9(mod 9)
   d) 10(mod 9).
6. The inverse of 7 modulo 26 is
   a) 12
   b) 14
   c) 15
   d) 20
7. The solution of the linear congruence 4x = 5(mod 9) is
   a) 6(mod 9)
   b) 8(mod 9)
   c) 9(mod 9)
   d) 10(mod 9)
8. The value of 5^{2003} mod 7 is
   a) 3

b) 4
c) 8
d) 9

9. The inverse of 3 modulo 7 is
a) -1
b) -2
c) -3
d) -4

10. The integer 2821 is a Carmichael number.
a) True
b) False

UNIT 2:

1. The linear combination of gcd(10 ,11) = 1 can be written as
a) (-1)*10 + 1*11
b) (-2)*10 + 2*11
c) 1*10 + (-1)*11
d) (-1)*10 + 2*11
2. The prime factorization of 7007 is _____
a) 7^3.11.13
b) 7^2.11.13
c) 7.11.13
d) 7.11^3.13
3. The greatest common divisor of $3^{13}.5^{17}$ and $2^{12}.3^5$ is _____
a) 3^0
b) 3^1
c) 3^3
d) 3^5
4. The greatest common divisor of 0 and 5 is _____
a) 0
b) 1
c) 2
d) 5
5. The lcm of 3 and 21 is _____ if gcd(3,21)=3.
a) 3
b) 12
c) 21
d) 42
6. If a|b and b|c, then a|c.
a) True
b) False
c) either

d) None of the above.

7. The integer 2821 is a Carmichael number.
a) True
b) False

8. Find the solution of x^2≡3 mod 23
a) x≡±16 mod 23
b) x≡±13 mod 23
c) x≡±22 mod 23
d) x≡±7 mod 23.

9. Find the solution of $x^2 \equiv 2 \bmod 11$ has a solution.
a) True
b) False

10. Find the solution of $x^2 \equiv 7 \bmod 19$
a) x≡±16 mod 23
b) x≡±11 mod 23
c) x≡±14 mod 23
d) x≡±7 mod 23.

UNIT 3:

1. What is 11 mod 7 and -11 mod 7?
a) 4 and 5
b) 4 and 4
c) 5 and 3
d) 4 and -4

2. The multiplicative Inverse of 24140 mod 40902 is
a) 2355
b) 5343
c) 3534
d) Does not exist

3. For the group Sn of all permutations of n distinct symbols,what is the number of elements in Sn?
a) n
b) n-1
c) 2n
d) n!

4. 7x = 6 mod 5. Then the value of x is
a) 2
b) 3
c) 4
d) 5

5. If gcd (2,3) = 1, then 2 divides 3. Is it true or **false?**

6. If a|b and b|c, then a|c.
   a) True
   b) False.

7. GCD (a,b) is the same as GCD(|a|,|b|).
   a) True
   b) False

8. Calculate the GCD of 8376238 and 1921023 using Euclidean algorithm.
   a) 13
   b) 12
   c) 17
   d) 7

9. 11^7 mod 13 =
   a) 3
   b) 7
   c) 5
   d) 15

10. What is 11 mod 7 and -11 mod 7?
    a) 4 and 5
    b) 4 and 4
    c) 5 and 3
    d) 4 and -4

Unit 4:

1. Calculate the GCD of 1160718174 and 316258250 using Euclidean algorithm.
   a) 882
   b) 770
   c) 1078
   d) 1225
2. The multiplicative Inverse of 1234 mod 4321 is
   a) 3239
   b) 3213
   c) 3242
   d) Does not exist
3. The multiplicative Inverse of 550 mod 1769 is
   a) 434
   b) 224
   c) 550
   d) Does not exist
4. The multiplicative Inverse of 24140 mod 40902 is
   a) 434
   b) 224
   c) 550
   d) Does not exist

5. [(a mod n) – (b mod n)] mod n = (b – a) mod n
   a) True
   b) False
6. Which of the following is a valid property for concurrency?
   a) a = b (mod n) if n|(a-b)
   b) a = b (mod n) implies b = a (mod n)
   c) a = b (mod n) and b = c (mod n) implies a = c (mod n)
   d) All of the mentioned
7. Calculate the GCD of 102947526 and 239821932 using Euclidean algorithm.
   a) 11
   b) 12
   c) 8
   d) 6
8. Calculate the GCD of 1160718174 and 316258250 using Euclidean algorithm.
   a) 882
   b) 770
   c) 1078
   d) 1225
9. [(a mod n) + (b mod n)] mod n = (b+a) mod n
   a) True
   b) False
10. If a|b and b|c, then a|bc.
   a) True
   b) False

Unit 5:

1. 11^7 mod 13 =
   a) 3
   b) 7
   c) 5
   d) 15

2. [(a mod n) – (b mod n)] mod n = (b – a) mod n
a) True
b) False

3. What is 11 mod 7 and -11 mod 7?
   a) 4 and 5
   b) 4 and 4
   c) 5 and 3
   d) 4 and -4

4. 11^7 mod 13 =
   a) 3
   b) 7
   c) 5
   d) 15

5. 7x = 6 mod 5. Then the value of x is
   a) 2
   b) 3
   c) 4
   d) 5

6. The greatest common divisor of 0 and 5 is _____
   a) 0
   b) 1
   c) 2
   d) 5

7. The lcm of 3 and 21 is _____ if gcd(3,21)=3.
   a) 3
   b) 12
   c) 21
   d) 42
8. The inverse of 4 modulo 7 is
   a) -1
   b) 0
   c) -3
   d) -4
9. The inverse of 2 modulo 7 is
   a) -1
   b) 2
   c) -3
   d) -4
10. The greatest common divisor of 7 and 5 is _____
   a) 0
   b) 1
   c) 2
   d) 5

K2 QUESTIONS:

UNIT 1:

1. Define Divisibility.
2. State unique factorization theorem.
3. Define Lucas number.
4. What is lattice point?
5. Define mathematical induction method.
6. State basic representation theorem.
7. What are the elementary properties of the function $\pi(x)$.
8. Define decimal notation with example.
9. Define binary notation with example.
10. What is the sum of the n consecutive number.

UNIT 2:

1) What is prime factorization?
2) What are Combinations?
3) Define Euler's function.
4) Define complete residue system.
5) Define reduced residue system.
6) Define " a congruent to b modulo c".
7) Define the fundamentals of congruence's.
8) What are the basic properties of congruence's
9) Define generating functions.
10) Define r – combination.

UNIT 3:

1) State Euclid's division lemma

2) What is integral combination of integers?

3) Define least common multiple

4) Define linear Diophantine equation

5) Define r-permutations.

6) Define residue of h modulo m.

7) Define polynomial congruences.

8) State Chinese remainder theorem.

9) Define mobius inversion formulae.

10) Define mobius pair.

UNIT 4:

1) Define Fermat's little theorem.

2) State Wilson's theorem.

3) State cancellation law.

4) What is reduced residue system?

5) What is linear congruences.

6) State Chinese remainder theorem.

7) What is Arithmetic function?

8) What is d(n) function?

9) What is $\sigma(n)$ function?

10) What is Mobius function

UNIT 5:

1) State Gold Bach conjecture.

2) What is multiplicative arithmetic function?

3) Define Mobius inversion formula.

4) Define mobius pair.

5) Define primitive roots.

6) What is greatest integer function?

7) Define Double dual.

8) Define prime number.

9) Write down the statement of unique factorization theorem.

10) Write down the statement of Wilson's theorem.

K3 QUESTIONS:

UNIT 1:

1. State and prove sum of the first n-positive integers is n(n+1)/2 .
2. Prove that $1^2+2^2+3^2+\ldots..+n^2 = n(n+1)(2n+1)/6$.
3. Prove that $1+3+5+\ldots.+(2n-1)=n^2$.
4. Prove that $1/2.1+1/2.3+1/2.4+\ldots.+1/n(n+1)=n/n+1$.
5. State and prove ,

   If x is any real number other than 1, then $\sum^{1} x^j = 1+x+x^2+\ldots.+x^{n-1}=x^n-1/x-1$.
6. Prove that $F_1+F_2+F_3+\ldots..+F_n = F_{n+2}-1$.
7. Prove that $F_1+F_3+F_5+\ldots.+F_{2n-1}=F_{2n}$.
8. Prove that $F_2+F_4+F_6+\ldots.+F_{2n}=F_{2n+1}-1$.
9. Prove that $F_1 F_2+F_2F_3+\ldots.+F_{2n-1}F_{2n} = (F_{2n})^2$.
10. Prove that $F_1F_2+F_2F_3+\ldots.+F_{2n}F_{2n+1}=(F_{2n+}1)^2-2$.

Unit-2:

1. If nPr denotes the numbers of r-permutations of the set S of objects then

   $nPr=n(n-1)\ldots.(n-r+1)$.
2. If nCr denotes the number of r-combinations taken from a set S of elements then,

   $({}^{n}c_r) = n(n-1)(n-2)\ldots.(n-r+1)/r!$.
3. If the product of any n-consecutive positive integer is divisible by the product of the first positive integers.
4. Prove that $({}^{n}_{r}) = ({}^{n}_{n-r})$.
5. Using the definition of $({}^{n}_{r})$ as the number of r-combination of a set S of n-elements . Prove combinationally $({}^{n}_{r}) = ({}^{n-1}_{r}) + ({}^{n-1}_{r-1})$.
6. Prove that , the Binomial theorem,

   $(x+y)^n = x^n + ({}^{n}_{1})\, x^{n-1} y + ({}^{n}_{2})\, x^{n-2} y^2 + \ldots.. + ({}^{n}_{n-1})\, xy^{n-1} + y^n$.
7. Prove that $2^n = 1+ ({}^{n}_{1}) + ({}^{n}_{2}) + \ldots.. + ({}^{n}_{n})$.
8. Prove that $1+ ({}^{n}_{2}) + ({}^{n}_{4}) + ({}^{n}_{6}) + \ldots\ldots=2^{n-1}$ and $({}^{n}_{1}) + ({}^{n}_{3}) + ({}^{n}_{5}) + ({}^{n}_{7}) + \ldots\ldots=2^{n-1}$.
9. Prove that $({}^{r}_{r}) + ({}^{r+1}_{r}) + ({}^{r+2}_{r}) + \ldots... + ({}^{r+m}_{r}) = ({}^{r+m+1}_{r+1})$.
10. Prove that if gcd(n,p)=1, then $p/n^{p-1}-1$.

Unit-3:

1. If d=gcd(a,c) then the congruence a.n ≡ b mod c has no solution if d doesn't divides b and it has d mutually incongruent solution , if d/b .

2. State and prove Wilson's theorem.

3. State and prove Chinese remainder theorem.

4. Prove that $1+a+a^2+\ldots.+a^{\phi(m)-1}= 0(\text{mod } m)$ if gcd(a,m)=1 and gcd(a-1,m)=1.

5. State and prove Euler's theorem.

6. If gcd(a,c)=1, then a has an inverse and it is unique modulo c.

UNIT-4

1. Prove that $\Sigma_{d/n}\phi(d)=n$.

2. Prove $\phi(n) = \Sigma_{d/n}\mu(d)n/d$.

$=n.\pi_{p/n}(1-1/p)$

3. If $n=P_1^{\rho 1}. P_2^{\rho 2}\ldots\ldots.. P_s^{\rho s}$ Prove that $\phi(n)=\phi(P_1^{\rho 1}). \phi(P_2^{\rho 2})\ldots\ldots\ldots.. \phi(P_s^{\rho s})$.

4. If $n_{1=}P_1^{\alpha 1}. P_2^{\alpha 2}\ldots\ldots\ldots.. P_s^{\alpha s}$,then $d(n)=d(P_1^{\alpha 1}).d(P_2^{\alpha 2})\ldots\ldots\ldots d(P_s^{\alpha s})$ And

$\sigma(n)= \sigma(P_1^{\alpha 1}). \sigma(P_2^{\alpha 2})\ldots\ldots\ldots \sigma (P_s^{\alpha s})$.

5. If $n_{=}P_1^{\alpha 1}. P_2^{\alpha 2}\ldots\ldots\ldots.. P_s^{\alpha s}$,then $d(n)= (\alpha_1+1). (\alpha_2+1)\ldots\ldots\ldots (\alpha_s+1)$ and

$\sigma(n)=P_1^{\alpha_1+1}-1/P_1-1. P_2^{\alpha_2+1}-1/P_s-1\ldots\ldots\ldots. P_s^{\alpha_s+1}-1/P_s-1$.

6. Prove that $\phi(n)$,d(n),$\sigma(n)$ and $\mu(n)$ are multiplicative arithmetic functions.

7. Prove that $\Sigma_{d/n}\ \mu(\alpha)= \begin{matrix} 1, & if & 1. \\ 0, & if & 1. \end{matrix}$

UNIT-5

1. Prove that $a^b \equiv 1(\text{mod } m)$ for some integer b, it is necessary and sufficient that gcd(a,m)=1.

2. If 'a' belongs to exponent h modulo m and $a^r\equiv 1(\text{mod } m)$ then h/r.

3. If g is primitive root modulo m, then $g,g^2\ldots\ldots.g^{\phi(n)}$ are mutually incongruent and form a reduced residue system modulo m.

4.If a belongs to the exponent h modulo m and gcd(k,h)=d,then a^k belongs to the exponent h/d modulo m.

5. If there exist any primitive root modulo m then there are exactly $\phi(\phi(m))$,mutually incongruent primitive roots.

6. For each prime P,there exist primitive root mod p.

7. Prove that $\lim_{\to\infty}\ x\ \infty$.

8. If k is any positive integer then, $x\ /x \leq \phi(k)/k + 2k/x$.

9. If m>1 and $P_{1,}P_2$……..P_s are all primes in {1,2,….m}then

$$\sum_{1}^{\frac{1}{}} \frac{1}{1-\frac{}{p}} \dots\dots\dots \frac{1}{1-\frac{}{ps}}.$$

10. If g is primitive root modulo m, then g,g^2…….$g^{\phi(n)}$ are mutually incongruent and form a reduced residue system modulo m.

THEORY OF NUMBERS

K4 QUESTIONS:

UNIT 1:

1. State and prove Euclid's division lemma .

2. If a and b are integers not both zero,then gcd(a,b) and is unique.

3. If a, b and c are integers, where a and c are relatively primes and if c/ab , then c divides b

4. The LDE ax+ by = c has a solution if d/c, where d=gcd(a,b) further move if (x_0 , y_0) is the Solution of this equation then the set of solution of the equation consist of all integers pair (x, y) where $x=x_0 + t.b/d$ and $y=y_0-t.a/d$, t=(…-2,-1,0,1,2,…)

5. State and prove Unique factorization theorem

UNIT 2:

1. If a,b,c,d are any integer ($c\neq0$) the following assertions hold .

   i). $a\equiv a \bmod c$,

   ii). $a\equiv b \bmod c$, then $b\equiv a \bmod c$

   iii). $a\equiv b \bmod c$ and $b\equiv a \bmod c$, then $a\equiv d \bmod c$.

2. State and prove cancellation law .

3. If S different integer $r_1,r_2,\ldots r_s$ form a complete residue system modulo m , then s=m.

4. If S integers $r_1,r_2,\ldots r_s$ form a reduced residue system modulo m , then $s=\phi(m)$.

5. Find integers r such that,

   i). $5x\equiv 4 \bmod 3$.

   ii). $7x\equiv 6 \bmod 5$.

   iii). $9x\equiv 8 \bmod 7$.

UNIT 3:

1. Prove that $L_n=L_{n-1}+L_{n-2}$, $(n\geq3)$.

2. Prove that $L_1+2L_2+4L_3+.....+2^{n-1}.L_n=2^n.F_{n+1}-1$.

3. State and prove Basis representation theorem .

4. State and prove Fermat's little theorem.

UNIT 4:

1. State and prove Mobius inversion formula.

2. State and prove Mobius pair.

3. $\{n,\phi(n)\},\{d/n,1\}$ and $\{\sigma(n),n\}$ are all Mobius pairs

UNIT 5:

1.Prove that $\lim_{x\to\infty} \frac{x}{x}$ 0.

2.If [x] denotes the largest integers that does not exceeded x then,$0\leq[2x]-2[x]\leq1$.

3.If P is a prime then $\sum^{\infty}$.(n/P_j) is the exponent of 'P' appearing in the prime factorisation of n factorial.

4.F(x)=x/log x, then F(x) is increasing for $x\geq\rho$,F(x-2)>1/2F(x) for $x\geq4k$ and (x+2/2)α15/16 $F(x)\geq8$.