|  |  |
| --- | --- |
| LOGO.jpg | **GEETHANJALIINSTITUTEOFSCIENCE&TECHNOLOGY**  (**ANAUTONOMOUSINSTITUTION**)  **(Approved by AICTE, New Delhi &Affiliated to JNTUA, Ananthapuramu) (Accredited by NAAC with “A” Grade, NBA (EEE,ECE &ME) &**  **ISO9001:2008CertifiedInstitution)** |
| **QUESTIONBANK(DESCRIPTIVE)**  **Subject Name with Code: NUMBER THEOREY AND ITS APPLICATION**  **Course & Branch:** B. Tech & CSE (CS)  **Year &Semester: II B. Tech II Semester**  **Regulation:RG23** | |

# UNIT-I

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **S. No** | **Question** | **[BT Level] [CO][**  **Marks]** | | |
| **2 Marks Questions (Short)** | | | | |
| **1.** | State the well-ordering property. | | L1, CO1, 2M | |
| **2.** | Find the values i) and ii) | | L3, CO1 , 2M | |
| **3.** | Convert (1894)10 from decimal to binary notation | | L3 ,CO1, 2M | |
| **4.** | State the division theorem. | | L1, CO1, 2M | |
| **5.** | Add (101111011)2 and (1100111011)2 | | L3, CO1, 2M | |
| **6** | Subtract (101110101)2 from (1101101100)2 | | L3, CO1, 2M | |
| **7** | Convert (A35B0F)16 to decimal notation | | L3, CO1, 2M | |
| **8** | Convert (2FB3)16to binary notation. | | L3, CO1, 2M | |
| **Descriptive Questions(Long)** | | | | |
| **1.** | Use mathematical induction to prove =1+2+3+…+n=(n(n+1))/2 | | | L3, CO1,10M |
| **2.** | Use mathematical induction to prove that = 12+22+32+ …..+n2  = (n(n+1)(2n+1)) /6 | | | L3, CO1,10M |
| **3.** | Let n and k be positive integers with n .  Prove that +(n=(  b) Find the values of i) ii) iii) 10c4 iv) 12c5 | | | L3, CO1,10M |
| **4.** | a)State and prove the division theorem.  b) Find the quotient and remainder in the division algorithm with divisor 17 and dividend 100 | | | L3, CO1,10M |
| **5.** | a) Convert (1864)10 and (2FB3)16to binary notation.  b) Convert (A35B0F)16 and (6105)7 to decimal notation | | | L3, CO1,10M |
| **6.** | a) Find gcd of 28 and 49, express it as linear combination of 28 and 49.  b) find the gcd ( 4340, 2821) by Euclidean algorithm and also express as GCD (4340,2821) = 2821x+4340y. | | | L3, CO1,10M |
| **7** | Show that event +ve integer can be written as the sum of distinct Fibonacci number | | | L3, CO1,10M |
| **8** | Find factor 6077 by using the method of Fermat factorization. | | | L3, CO1,10M |
| **9** | Find all integer solutions of linear Diophantine equation 2x+3y+4z=5. | | | L3, CO1,10M |
| **10** | Find all integer solutions of systems of linear Diophantine equation  x +y +z =100, x+8y+50z =156. | | | L3, CO1,10M |

# UNIT-II

|  |  |  |  |
| --- | --- | --- | --- |
| **S.No**  **.** | **Question** | | **[BTLevel][CO][**  **Marks]** |
| **2MarksQuestions (Short)** | | | |
| **1.** | Write the first five Fibonacci numbers. | L2,CO2,2M | |
| **2.** | State the fundamental theorem of arithmetic | L2,CO2,2M | |
| **3.** | Find the prime factorization of the positive integers 222 and 5040 | L2,CO2,2M | |
| **4.** | Find gcd ( 45,75,25) | L2,CO2,2M | |
| **5.** | Define linear Diophantine equation in two variables with example | L3,CO2,2M | |
| **6** | Find the G.C.D of 6,10,15 | L3,CO2,2M | |
| **7** | State Euclidean algorithm | L3,CO2,2M | |
| **8** | State fermats factorization theorem | L3,CO2,2M | |
| **DescriptiveQuestions(Long)** | | | |
| **1.** | a)find the least positive residue of mod 645  b) find the least positive residue of (mod11) | | L3, CO2, 10M |
| **2.** | find the all solutions 9x ≡ 12(mod15)  find the values of x, 2x ≡ 3 (mod 8) | | L3,CO2,10M |
| **3.** | solve the systems of linear congruence’s  x ≡ 1 (mod3), x ≡ 2(mod5), x ≡ 3(mod7) | | L3, CO2,10M |
| **4.** | solve the systems of linear congruence’s  x ≡ 2 (mod3), x ≡ 3(mod5), x ≡ 2 (mod7) | | L3, CO2,10M |
| **5** | solve 2x≡ 1(mod 3) ,2x ≡ 2 (mod4), x≡ 3(mod5 ) using c.r.t method | | L3, CO2,10M |
| **6** | find the solutions of the congruence’s  x≡ 4 (mod 11) ,x≡ 3( mod 17)  solve the system of congruences  x ≡ 1 (mod 3) , x ≡ 2 (mod 6 ), x ≡ 3 (mod7 ) by iterative method | | L3, CO2,10M |
| **7.** | system of congruences x ≡ 3 ( mod 7) , x ≡ 4 (mod 11 ), x ≡ 5 (mod13) to solve of congruences using c. r.t . method | | L3, CO2,10M |
| **8.** | solve the system of liner congruences 3x+4y ≡ 5 (mod 13),  2x+5y ≡ (mod13) | | L3, CO2,10M |
| **9.** | a) Find an inverse modulo 5 of .  b) Find an inverse modulo 7 of | | L3,CO2,10M |
| **10.** | Find the solution of the system of linear congruence’s 2x+3y≡5 (mod 7), x+5y ≡6 (mod 7). | | L3,CO2,10M |
| **11.** | Find the all the solutions of system of linear congruence’s equations  2x1+5x2+6x3 = 3 mod(7) , 2x1+x3 = 4 mod(7) , x1+2x2+3x3 = 1mod(7) | | L3,CO2,10M |

# UNIT-III

|  |  |  |
| --- | --- | --- |
| **S.No**  **.** | **Question** | **[BTLevel][CO][**  **Marks]** |
| **2MarksQuestions (Short)** | | |
| **1.** | Show that 125671221 is divisible by 9 | L3,CO3,2M |
| **2.** | Show that the number 1571427 is divisible by 11 . | L3,CO3,2M |
| **3.** | State Wilson’s Theorem | L3,CO3,2M |
| **4.** | State Fermat’s Little Theorem | L3,CO3,2M |
| **5.** | Define Carmichael number | L3,CO3,2M |
| **6** | Write about round robin tournament | L3,CO3,2M |
| **7** | Define congruence with an examples | L3,CO3,2M |
| **8** | State chimes remainder theorem | L3,CO3,2M |
| **Descriptive Questions(Long)** | | |
| **1.** | Explain the perpetual calendar. Write algorithm to determine the day of the week on 13 January in 2020 | L3,CO3,10M |
| **2.** | Explain Round – Robin tournament and write an algorithm a Round – Robin tournament schedule for 7 – teams | L3, CO3,10M |
| **3.** | State and prove Wilson’s Theorem | L2,CO3,10M |
| **4.** | State and prove Fermat’s Little theorem | L2, CO3,10M |
| **5.** | a) if p is a prime and a is a positive integer then a p = a mod(p)  b) using Fermat’s little theorem find the least positive residue of 21000000  mod (17) | L3, CO3,10M |
| **6.** | Using Fermat’s Little theorem find the solutions of linear congruence’s   1. 7x = 12 mod(17) , ( ii ) 4x =11 mod(19) | L3,CO3,10M |
| **7.** | Define Carmichael number and the integer 561 is Carmichael number | L3,CO3,10M |
| **8.** | a) state and prove Euler’s theorem  b) find the solution of 3x =7 mod(10) | L3,CO3,10M |
| **9.** | Define locals – larcener test , and show that M7 is a prime using locals- larcener test | L3, CO3,10M |
| **UNIT-IV** | | |
| **S.No**  **.** | **Question** | **[BTLevel][CO][**  **Marks]** |
| **1** | State Euler’s theorem | L3, CO4,2M |
| **2** | State the Gauss lemma | L3, CO4,2M |
| **3** | Write formula for (q/p) in legendry symbol | L2, CO4,2M |
| **4** | Write gauss lemma in number theorey | L2, CO4,2M |
| **5** | State the quadratic reciprocity . | L2, CO4,2M |
| **6** | Define Carmchael number with an example | L2, CO4,2M |
| **7** | Define perfect number | L2, CO4,2M |
|  | | |
| **1.** | If P is an an odd prime , then there are exactly (p – 1 ) / 2 quadratic residues of p and (p – 1 ) / 2 quadratic non residue of p among the integers 1,2,3,...........(p -1) | L3,CO4,10M |
| **2.** | State and prove Euler’s criterion | L3,CO4,10M |
| **3.** | Let p be an odd prime a and b are two integers not divisible by p then   1. a = b mod (p) then [a/p] = [ b / p] 2. [a/p] [ b / p] = [ a b /p ] 3. [ a2/p] = 1 | L3,CO4,10M |
| **4.** | If p is an odd prime then [ 2 /p ] = (-1)( p2-1) /8 hence 2 is a quadratic residue of all primes, p = + 1mod(8) and quadratic non residue of primes p = +3 mod(8) | L3,CO4,10M |
| **5.** | State and prove law of quadratic reciprocity | L3,CO4,10M |
| **6.** | a) find the Legendre symbol (889/50261)  b) Evaluate 1001/ 9907 | L3,CO4,10M |
| **7.** | a)Find the all solutions of quadratic congruence’s x2 +7x+10 = 0 mod(11)  b) Find the all solutions of quadratic congruence’s x2 +x+1 = 0 mod(7) | L3,CO4,10M |
| **8.** | a) To test whether the congruence’s x2 = -38 (mod13) is solvable or not  b) To test whether x2 = 196 mod11357 has solutions( or) not | L3,CO4,10M |
| **9.** | a)Find the factor of n = 1111 using f(x) = x2+1 and x0 = 2  b) a)Find the factor of n = 1189 using f(x) = x2+1 and x0 = 1 | L3,CO4,10M |
|  | **Unit-5** |  |
| **S. No** | **Question** | **[BTLevel][CO][**  **Marks]** |
| **2MarksQuestions (Short)** | | |
| **1** | What is meant by Cryptography | L2, CO5,2M |
| **2** | Define Encryption and decryption | L2, CO5,2M |
| **3** | What is meant by Cryptanalysis? | L2, CO5,2M |
| **4** | Explain about Knapsack ciphers | L2, CO5,2M |
| **5** | Explain about Caesar cipher | L2, CO5,2M |
| **6** | Write any two goals of cryptpgraphy | L2, CO5,2M |
| **7** | what do mean about by probabilistic encryption | L2, CO5,2M |
| **8** |  |  |
| **Descriptive Questions(Long)** | | |
| **1** | What is a Cipher? Explain types of Ciphers | L2,CO5,10M |
| **2** | Explain about Character Cipher? What are the types of Character Ciphers | L3,CO5,10M |
| **3** | What is Block Cipher? Explain Block Cipher Modes of Operation | L3,CO5,10M |
| **4** | Explain how to encipher and decipher the messages using Block cipher | L3,CO5,10M |
| **5** | What is discrete logarithmic problem and explain it. | L3,CO5,10M |
| **6** | Explain in detail about the RSA Cryptosystem. | L3,CO5,10M |
| **7** | Explain about various encryption mechanisms | L3,CO5,10M |
| **8** | Discuss about the following   1. Caesar cipher ii) Block ciphers | L3,CO5,10M |
| **9** | Discuss About Public-Key Cryptography | L3,CO5,10M |
| **10** | Illustrate the Knapsack ciphers | L3,CO5,10M |

: