Model Question Paper -1 (CBCS Scheme)

USN										

Fourth Semester B.E Degree Examination

NUMBER THEORY (BCY405D)

TIME: 03 Hours **Max.Marks:100**

Note: (i) Answer any **FIVE** full questions, choosing at least **ONE** question from each **MODULE.**
(ii) Statistical tables and Mathematics Formula handbooks are allowed**.**

		Module -1	M	L	C
Q.01	a	Apply the concept of Euclid's Algorithm to find the GCD of 385 and 792, and hence express it in the form of $385x + 792y$	**6**	**L2**	**CO1**
	b	.Find the unit digit for the following by applying congruence 2^{2013}	**7**	**L2**	**CO1**
	c	Solve by applying Chinese Remainder theorem $x \equiv 2 \pmod 3$, $x \equiv 3 \pmod 5$, $x \equiv 2 \pmod 7$	**7**	**L3**	**CO1**
		OR			
Q.02	a	Apply the concept of Euclid's Algorithm to find the GCD of 25520 and 19314.	**6**	**L2**	**CO1**
	b	Find the remainder when $135 \times 74 \times 48$ divided by 7 by applying congruence	**7**	**L2**	**CO1**
	c	Analyze "If a cock is worth 5coins, a hen 3 coins and three chicks 1coin, how many cocks, hens and chicks, totaling100, can be brought for 100 coins by using linear Diophantine equation?	**7**	**L3**	**CO1**
		Module-2			
Q.03	a	Find the remainder when 3^{31} is divided by 7 by applying Fermat's little theorem.	**6**	**L2**	**CO2**
	b	Find the remainder when 23^{130} is divided by 25 by applying Euler's Totient function	**7**	**L2**	**CO2**
	c	Apply the method of Linear Congruent Generator method to generate the sequence of pseudo random numbers when $X_0 = 3$, $a = 5$, $b = 1$ and $m = 8$ given. Hence find period and random variate of the sequence.	**7**	**L3**	**CO2**
		OR			
Q.04	a	Find the remainder when 13^{55} is divided by 17 by applying Fermat's little theorem.	**6**	**L2**	**CO2**
	b	Find the remainder when $12 \times 13 \times 14$……..$\times 21$ is divided by 11 by applying Wilson's theorem.	**7**	**L1**	**CO2**

	c	The random sequence of 73 observations are 49, 95, 82 ,19 ,41, 31, 12, 53, 62, 40, 87, 83, 26, 1, 91, 55, 38, 75, 90, 35, 71, 57, 27, 85, 52, 08, 35, 57, 88, 38, 77, 86, 29, 18, 09, 96, 58, 22, 08, 93, 85, 45, 79, 68, 20, 11, 78, 93, 21, 13, 06, 32, 63, 79, 54, 67, 35, 18, 81, 40, 62, 17, 76, 74, 76, 45, 29, 36, 80, 78, 95, 25, 52. Apply chi-square test for randomness at $(\chi^2_{\alpha=0.005} = 16.919 \text{ at dof } 9)$	**7**	**L3**	**CO2**
Module-3					
Q.05	a	Find the order of 8 modulo13 By applying the concept of " Order of an Integer Modulo 'n' .	**6**	**L1**	**CO3**
	b	If P = 13 is prime then show that $P - 1 = \sum \psi(d)$	**7**	**L3**	**CO3**
	c	Apply the method of quadratic congruence with composite moduli, solve the $x^2 \equiv 23 \pmod{7^2}$	**7**	**L3**	**CO3**
OR					
Q. 06	a	Show that 2 is a primitive root of 5 but not of 13.	**6**	**L1**	**CO3**
	b	Find the values of 'x' for $x^2 + 3x + 11 \equiv 0 \pmod{13}$ by applying the concept of quadratic congruence.	**7**	**L3**	**CO3**
	c	Applying generalized quadratic reciprocity law to determine weather the following congruence $x^2 \equiv 196 \pmod{1357}$ with composite modulus are solvable? If yes find 'x' values	**7**	**L3**	**CO3**
Module-4					
Q. 07	a	Evaluate 111/ 1001 by using Jacobi symbol	**6**	**L2**	**CO4**
	b	Prove that the Fermat's number $F_5 = 2^{2^5} + 1$ is divisible 641	**7**	**L2**	**CO4**
	c	Convert $\sqrt{2}$ into simple continued fractions .	**7**	**L3**	**CO4**
OR					
Q.08	a	Whether the congruence $x^2 \equiv 20 \pmod{31}$ is solvable using Legendre symbol?	**6**	**L2**	**CO4**
	b	Find all Pythagorean triangles whose areas are equal to their perimeter.	**7**	**L2**	**CO4**
	c	Determine the rational numbers for [0; 1, 2, 3, 4, 3, 2, 1] to simple continued fractions	**7**	**L3**	**CO4**
Module-5					
Q. 09	a	On the elliptic curve $y^2 = x^3 + 8$, Compute P+P where P=(1, 3)	**10**	**L3**	**CO5**

	b	On elliptic curve $y^2 = x^3 + 5x + 2\ (mod 11)$ with P= (9, 3) and Q(4, 3), Find P+Q, 2P and 2Q.	**10**	**L3**	**CO5**
OR					
Q.10	a	Generate first five rational points on the unit circle by using one rational point.	10	**L3**	**CO5**
	b	Find all possible points on elliptic curve $y^2 = x^3 + 3x + 4\ (mod 7)$.	**10**	**L3**	**CO5**

Model Question Paper - 2 (CBCS Scheme)

USN										

Fourth Semester B.E Degree Examination

NUMBER THEORY (BCY405D)

TIME: 03 Hours **Max.Marks:100**

Note: (i) Answer any **FIVE** full questions, choosing at least **ONE** question from each **MODULE.**
(ii) Statistical tables and Mathematics Formula handbooks are allowed**.**

		Module -1	M	L	C
Q.01	a	Apply the concept of Euclid's Algorithm to find the GCD of 54 and 7 and express it in the form of $54x + 7y$.	**6**	**L2**	**CO1**
	b	Find the least positive value of 'x' for the following by applying congruence $96 \equiv x/7 \pmod 5$.	**7**	**L2**	**CO1**
	c	Find the general solution of linear Diophantine equation 172x+20y = 1000 using Euclidian algorithm to find GCD and also find solution in the positive integer.	**7**	**L3**	**CO1**
		OR			
Q.02	a	Find the remainder when 2^{23} is divided by 47 by applying congruence	**6**	**L2**	**CO1**
	b	Find x for the following by applying linear congruence $14x \equiv 12 \pmod{18}$	**7**	**L2**	**CO1**
	c	Solve by applying Chinese Remainder theorem $x \equiv 5 \pmod 3$, $x \equiv 2 \pmod 5$, $x \equiv 1 \pmod{11}$	**7**	**L3**	**CO1**
		Module-2			
Q.03	a	Find the remainder when 128^{129} is divided by 17 by applying Fermat's little theorem.	**6**	**L2**	**CO2**
	b	Simplify 146! is divided by 149 by using Wilson's theorem	**7**	**L2**	**CO2**
	c	The random sequence of numbers 0.44, 0.81, 0.14, 0.05 and 0.93 has been generated, check the uniformity at $\alpha = 0.05$ by applying the Kolmogrov-Smirnov test $(D_{\alpha} = 0.565)$	**7**	**L3**	**CO2**
		OR			
Q.04	a	Find the remainder when 3^{100000} is divided by 53 by applying Fermat's little theorem.	**6**	**L2**	**CO2**
	b	Find the remainder when 7^{30} is divided by 15 by applying Euler's Totient function	**7**	**L1**	**CO2**

	c	Apply the method of Linear Congruent Generator method to generate the sequence of pseudo random numbers when X_0 =27, a = 17, b = 43 and m= 100 given. Hence find random bit sequence, period and random variate of the sequence.	**7**	**L3**	**CO2**
Module-3					
Q.05	a	Find the order of the integer 2 and 5 at modulo 17	**6**	**L1**	**CO3**
	b	Find the quadratic residue and non quadratic residue of 13 by applying Euler's Criterion	**7**	**L3**	**CO3**
	c	Applying generalized quadratic reciprocity law to determine weather the congruence $x^2 \equiv 231 \pmod{1105}$ with composite modulus are solvable?	**7**	**L3**	**CO3**
OR					
Q. 06	a	Apply the concept of primitive root to show that 2 is a primitive root of 5 but not of 13	**6**	**L1**	**CO3**
	b	Prove that " For K ≥ 3 the integer 2^k has no primitive roots"	**7**	**L3**	**CO3**
	c	Apply the method of quadratic congruence with composite moduli, Solve the $x^2 \equiv 14 \pmod{5^2}$.	**7**	**L3**	**CO3**
Module-4					
Q. 07	a	Whether the congruence $x^2 \equiv -46 \pmod{17}$ is solvable using Legendre symbol?	**6**	**L2**	**CO4**
	b	Apply Pepin's test " For n≥1; the Fermat numbers $F_n = 2^{2^n} + 1$ is prime iff $3^{\frac{(F_n-1)}{2}} \equiv -1 \ (mod F_n)$.	**7**	**L2**	**CO4**
	c	Compute the convergents of [1; 2, 3, 3, 2, 1] to simple continued fractions.	**7**	**L3**	**CO4**
OR					
Q.08	a	Using the Jacobi symbol determine whether the $x^2 \equiv 231 \pmod{1105}$ is solvable.	**6**	**L2**	**CO4**
	b	Find all Pythagorean triple whose terms form an arithmetic progression.	**7**	**L2**	**CO4**
	c	Evaluate $\lim_{k\to\infty} \frac{F_{k+1}}{F_k}$ where F_k is K^{th} Fibonacci number.	**7**	**L3**	**CO4**
Module-5					
Q. 09	a	On the elliptic curve $y^2 = x^3 - 5x$, Let P=(-1, 2) and Q(0,0), find P+Q and 2P.	**10**	**L3**	**CO5**
	b	Write the " Diffie – Hellman key exchange algorithm" by using Elliptic curve cryptography.	**10**	**L3**	**CO5**
OR					

Q. 10	a	On the elliptic curve $y^2 = x^3 - 5x$, Let P=(-1, 2) and Q(0,0), find P+Q and 2P.	**10**	**L3**	**CO5**
	b	On elliptic curve $y^2 = x^3 + 3x + 4\ (mod 7)$ with P= (1, 1) and Q(2, 5), Find P+Q and double the point (2, 2) = R	**10**	**L3**	**CO5**