TOTAL PAGES : 2

22MAP315BN

PSG COLLEGE OFARTS & SCIENCE
(AUTONOMOUS)

MSc DEGREE EXAMINATION MAY 2025
(Third Semester)

Branch - **MATHEMATICS**

MAJOR ELECTIVE COURSE – II: NUMBER THEORY AND CRYPTOGRAPHY

Time: Three Hours Maximum: 75 Marks

SECTION-A (10 Marks)
Answer **ALL** questions
ALL questions carry **EQUAL** marks (10 × 1 = 10)

Question No.	Question	K Level	CO
1	a is a proper divisor of b if _____. (a) $a\|b$ (b) $a\|b$ *and* $a<b$ (c) $b\|a$ *and* $b<a$ (d) $a<b$	K1	CO1
2	If c|a and c|b, then c is a _____ of a and b. (a) divisor (b)greatest common divisor (c) common divisor (d) proper divisor	K2	CO1
3	A natural number, p is said to be _____ number if it has a non-trivial divisor d, such that 1<d<n. (a) composite (b) real (c) rational (d) prime	K1	CO2
4	If _____, then n has a prime factor, p. (a) n=1 (b) n=0 (c) n<1 (d) n>1	K2	CO2
5	If a ≡ b(mod m) and n|m, then _____. (a) $ac \equiv bc(mod\ m)$ (b) $a \equiv b(mod\ n)$ (c) $a \equiv bc(mod\ m)$ (d) $a \equiv b(mod\ cm)$	K1	CO3
6	A _____ of a non empty set is a collection of one or more subsets of S such that each element of S belongs to precisely one subset. (a) set (b) congruence (c) partition (d) relation	K2	CO3
7	τ(n) is _____. (a) associate (b) commutative (c) multiplicative (d) zero	K1	CO4
8	m is prime if and only if σ(m)=_____. (a) m (b) m+1 (c) m+2 (d) 0	K2	CO4
9	The process of converting a plain text to cipher text is called _____. (a) transformation (b) encryption (c) decryption (d) retrieval	K2	CO5
10	In public key cryptography, the public key is used for _____. (a) encrypting messages (b) decrypting messages (c) generating the private key (d) signing messages	K2	CO5

SECTION - B (35 Marks)
Answer **ALL** questions
ALL questions carry **EQUAL** Marks (5 × 7 = 35)

Question No.	Question	K Level	CO
11.a.	(i) If the integers a and b have the same parity, then prove that a+b is even. (ii) If ab is odd, then prove that a and b are both odd.	K3	CO1
	(OR)		
11.b.	Find x and y such that (87,27)=87x+27y.		
12.a.	Prove that there exists infinitely many primes of the form 4k-1.	K3	CO2
	(OR)		
12.b.	Prove that there exist arbitrarily large gaps between consecutive primes.		

Cont...

13.a.	Let m be a natural number. Then prove that the congruence (mod m) is an equivalence relation on Z.	K3	CO3
	(OR)		
13.b.	Prove that the congruence $ax \equiv b(mod\ m)$ has atleast one solution if and only if (a,m)|b.		
14.a.	If f and g are both multiplicative functions, the prove that f*g is also a multiplicative function.	K3	CO4
	(OR)		
14.b.	Let h=f*g. If g and h are both multiplicative and neither g nor h is the zero function, then prove that f is also multiplicative.		
15.a.	Given the cipher text "WKNCCHSSJH" and knowing the plain text begins with "GIVE". Find the deciphering matrix A^{-1} and use it to decode the entire message.	K2	CO5
	(OR)		
15.b.	Explain Knapsack problem and its significance in cryptography.		

SECTION -C (30 Marks)

Answer **ANY THREE** questions
ALL questions carry **EQUAL** Marks (3 × 10 = 30)

Question No.	Question	K Level	CO
16	(i) State and prove Euclid's lemma. (ii) Prove that $2^n > n$ for every natural number n.	K3	CO1
17	State and prove fundamental theorem of arithmetic.	K3	CO2
18	State and prove Fermat's Little theorem.	K3	CO3
19	State and prove Euler's theorem.	K3	CO4
20	Discuss the algorithms for finding discrete logs in finite fields.	K2	CO5

Z-Z-Z END