22MAP315BN

PSG COLLEGE OF ARTS & SCIENCE
(AUTONOMOUS)

MSc DEGREE EXAMINATION DECEMBER 2025
(Third Semester)

Branch - **MATHEMATICS**

MAJOR ELECTIVE COURSE – II: NUMBER THEORY & CRYPTOGRAPHY

Time: Three Hours | Maximum: 75 Marks

SECTION-A (10 Marks)

Answer **ALL** questions
ALL questions carry **EQUAL** marks (10 × 1 = 10)

Module No.	Question No.	Question	K Level	CO
1	1	G.C.D of 87,27 is _____ a) 3 b) 4 c) 1 d) 5	K1	CO1
	2	L.C.M of 418,165 is _____ a) 6207 b) 1440 c) 6270 d) 6543	K2	CO1
2	3	Prime Counting Function $\pi(37)$ = _____ a) 2 b) 6 c) 8 d) 10	K1	CO2
	4	If (a,b) = 1, then there are infinitely many primes of the form_____ a) an+b b) an-3b c) 2an-2b d) an^2-b	K2	CO2
3	5	If p is prime and (a,p)= _____, then $a^{p-1} \equiv 1 \pmod p$ a) 3 b) 1 c) 5 d) 7	K1	CO3
	6	Let p be an odd prime. Then $x^2 \equiv a^2 \pmod p$ if and only if $x \equiv$ ___ (mod p) a) -1 b) 0 c) ±a d) 1	K2	CO3
4	7	Sum of divisors of n, $\sigma(6)$=_____ a) 12 b) 14 c) 16 d) 18	K1	CO4
	8	If p and q are primes such that q =_____ where q is Mersenne number. a) 2^{p+1}-1 b) 2^p-1 c) 2^p-2 d) 1-2^p	K2	CO4
5	9	The _____ cryptosystem is an early public-key algorithm based on the computationally difficult subset-sum problem. a) RSA b) Knapsack c) Diffie-Hellman d) Elgamal	K1	CO5
	10	_____ key cryptography, also known as symmetric-key cryptography, uses a single, secret key for both encrypting and decrypting a) Private b) Public c) Zero sum d) transition	K2	CO5

Cont...

SECTION - B (35 Marks)

Answer **ALL** questions

ALL questions carry **EQUAL** Marks (5 × 7 = 35)

Module No.	Question No.	Question	K Level	CO
1	11.a.	Prove that $F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta}$.	K1	CO1
		(OR)		
	11.b.	Find x, y such that (87,27) = 87x+27y.		
2	12.a.	If n is composite, and if p is the least prime factor of n, then prove that $p \le \sqrt{n}$.	K4	CO2
		(OR)		
	12.b.	If n > 1, then prove that the canonical factorization of n is unique.		
3	13.a.	State and prove Chinese Remainder Theorem.	K3	CO3
		(OR)		
	13.b.	State and prove Wilson's theorem.		
4	14.a.	If f is an arithmetic function such that $f(1) \neq 0$, then prove that f^{-1} exists.	K6	CO4
		(OR)		
	14.b.	If p is an odd prime and (a,p)=1, then prove that $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod p$.		
5	15.a.	Find the inverse of $A = \begin{pmatrix} 2 & 3 \\ 7 & 8 \end{pmatrix} \in M_2(Z/26Z)$	K5	CO5
		(OR)		
	15.b.	Explain ElGamal cryptosystem.		

SECTION -C (30 Marks)

Answer **ANY THREE** questions

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

Module No.	Question No.	Question	K Level	CO
1	16	(i)If ab=4k-1, then prove that a=4m-1 for some m or b=4n-1for some n. (ii) State and prove Euclid's Lemma.	K3	CO1
2	17	For any natural number, n, prove that $n! = \prod p^{\sum k \ge 1 \left[\frac{n}{p^k}\right]}$ the product being taken over all primes.	K4	CO2
3	18	(i) Solve the congruence $x^3 - 5x + 1 \equiv 0 \pmod{27}$. (ii) If p is an odd prime, $p \mid (a^2 + b^2)$, and $(a,b) = 1$, then prove that p≡1(mod 4).	K5	CO3
4	19	State and prove Euler's theorem.	K2	CO4
5	20	Suppose we known that our adversary is using an enciphering matrix A in the 26-letter alphabet. We intercept the ciphertext "WKNCCHSSJH" and we know that the first word is "GIVE" We want to find the deciphering matrix A^{-1} and read the message.	K6	CO5

Z-Z-Z END