A
00I-A1SQ2

0200MAT266042502

Pages: 3

Reg No.:_______________ Name:_______________

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

B.Tech Degree S4 (S,FE) Examinations May 2026 (2019 Scheme)

Course Code: MAT266

Course Name: MATHEMATICAL FOUNDATIONS FOR SECURITY SYSTEMS

Max. Marks: 100 Duration: 3 Hours

PART A

(Answer all questions; each question carries 3 marks)

		Marks
1	Construct the addition and multiplication tables for the ring $< \mathbb{Z}_6, +, \cdot >$ and identify the units and zero divisors.	3
2	What can you say about the characteristics of a field? Which field is contained in any field of characteristic zero?	3
3	Let $\mathbb{F}_2 = \{0,1\}$ be the field containing two elements. Check whether the vectors $v_1 = \begin{bmatrix}1\\1\\0\end{bmatrix}, v_2 = \begin{bmatrix}0\\1\\1\end{bmatrix}, v_3 = \begin{bmatrix}1\\0\\1\end{bmatrix}$ are linearly independent in ${\mathbb{F}_2}^3$.	3
4	Is 3 a primitive element of $GF(7)$.	3
5	Define $\pi(n)$, for a positive integer n. Find an approximation of $\pi(100000)$.	3
6	Let n be a positive integer. Find the $\gcd(3n + 1, 2n + 1)$.	3
7	Find the Quadratic residues and the Quadratic non-residues of the set ${Z_{11}}^*$.	3
8	Find the order of all elements in ${Z_{10}}^*$.	3
9	The mean and variance of a binomial random variable X are 48 and 12 respectively. Find $P(X = 0)$.	3
10	Suppose that the number of items produced in a factory during a week is a random variable with mean 500. What can be said about the probability that this week's production will be at least 1000?	3

PART B

(Answer one full question from each module, each question carries 14 marks)

Module -1

11	a)	Construct the addition and multiplication tables for the quotient ring $Q = \mathbb{Z}_2[x]/< x^2 + x + 1 >$. Is it a field? Justify your answer	7
	b)	Define a field and a finite field. Give one example for each.	7

12 a) Consider the primitive polynomial $g(x) = x^3 + x^2 + 1$ over $GF(2)$. Construct the extension field $GF(2^3)$. 7

b) Construct the subfield structure of the Galois field $GF(3^{24})$ 7

Module -2

13 a) Show that the polynomial $p(x) = x^3 + x^2 + 1$ is primitive in $GF(2)[x]$. 7

b) Consider $\mathbb{R}^4$ with $v_{1=(1,-1,3,1)}, v_{2=(-1,1,2,4)}, v_{3=(1,-2,-2,3)}$. Check whether they are linearly independent. 7

14 a) Check whether set of all points on the plane $2x - y + 3z = 0$ is a subspace of R^3 under standard operations. 7

b) Find a basis and the dimension for the orthogonal complement of the vector subspace spanned by the set of vectors $\{(1,1,1,0,0), (0,1,1,1,0), (0,0,1,1,1)\}$ in $\mathbb{R}^5$. 7

Module -3

15 a) Using Extended Euclidean algorithm, express gcd(320,84) as a linear combination of 320 and 84. 7

b) Describe Extended Euclidean Algorithm. 7

16 a) State Fermat's Little Theorem. Compute (a) $15^{18} (mod\ 17)$, (b) $5^{-1} (mod\ 23)$. 7

b) Find the result of the following using Euler's theorem, 7

(i) 111^{120} mod 100 (ii) 11^{-1} mod 100

Module -4

17 a) State Chinese Remainder Theorem. Solve the simultaneous equations $x \equiv 1(mod 3)$, $x \equiv 2(mod\ 5)$, $x \equiv 3(mod\ 7)$ using Chinese Remainder Theorem. 7

b) For which value of n does the group $G = < z_n^*, \times >$ have primitive roots, $(a)\ 17$ $(b)\ 50$. Also find the no of primitive roots of each group. 7

18 a) Describe probabilistic algorithms. Determine whether 27 pass Miller Rabin Primality test. 7

b) Using Pollard rho method, factorize $n = 1111$ using the function $f(x) = x^2 + 1$ and the seed $x_0 = 2$. 7

Module -5

19 a) Let X be a discrete random variable with the following probability mass function 7

$P(X = 1) = 0.3, P(X = 2) = 0.2, P(X = 3) = 0.1, P(X = 4) = 0.4$

(i) Verify that this function satisfies the properties of a PMF.

(ii) Calculate the probability that X is an even number.

(iii) Determine the cumulative distribution function (CDF) of X.

b) A manufacturer claims that at most 10% of his product is defective. To test this claim, 18 units are inspected and his claim is accepted if among these 18 units at most 2 are defective. Find the probability that the manufacturer's claim will be accepted if the actual probability that a unit is defective is 0.05. 7

20 a) A random variable X has the following probability distribution: 7

X	-2	-1	0	1	2	3
P(x)	0.1	$15k^2$	0.2	2k	0.3	3k

(i) Find the value of k (ii) the mean and variance of X.

b) Derive the mean and variance of Binomial distribution. 7

***