Yashoda Shikshan Prasarak Mandal's
YASHODA TECHNICAL CAMPUS, SATARA
FACULTY OF ENGINEERING
NH-4, Wadhe Phata, Satara., Tele Fax- 02162-271238/39/40
Website- www.yspmsatara.co.in Email-admin@yspmsatara.co.in
Approved by AICTE- New Delhi, Govt. of Maharashtra (DTE, Mumbai) Affiliated to DBATU Lonere.
DEPARTEMENT OF COMPUTER SCIENCE AND ENGINEERING

Class: FY. M tech CSE

Subject: Applied Mathematics and number Theory

CA 1:- Statistical & Probability Model example based Case Study
Mode: Written, solve on journal page and submit + Explanations

1. Case Study: Spam Detection Using Bayes' Theorem
Using P(Spam)=0.30, P("Offer"|Spam)=0.8, P("Offer"|Not Spam)=0.1, compute probability an email with 'Offer' is spam. Explain Bayes' role.
2. Case Study: Poisson Model for Server Failures
Average 4 failures/week. Find probability of exactly 6 failures and zero failures using Poisson distribution.
3. Case Study: CPU Queueing (M/M/1)
Arrival rate λ=5/s, service rate μ=8/s. Find utilization, avg number in system, avg waiting time.
4. Case Study: Markov Chain for Website Navigation
States: Home, Products, Cart. Given transition probabilities, compute probability of reaching Cart in 2 steps starting from Home.
5. Case Study: A/B Testing (Hypothesis Test)
200 users saw A (40 clicked), 250 saw B (75 clicked). Perform proportion Z-test at 5% level.
6. Case Study: ML Classification Metrics
Given TP=70, FP=30, TN=90, FN=10 compute accuracy, precision, recall, F1-score.
7. Case Study: Sensor Noise (Normal Distribution)
Sensor: mean=40°C, SD=3°C. Find probability readings between 38–44°C and >45°C.
8. Case Study: Linear Regression House Pricing
Model: Price = 25,000×Area + 3,00,000. Predict price for 1800 sq.ft.
9. Case Study: Monte Carlo Simulation for Stock Forecasting
Given μ=0.002, σ=0.03. Explain steps to simulate 10 random stock price paths.
10. Case Study: Software Reliability (Kaplan–Meier)
Failure times: 12,15,20,28,34,40. Compute KM reliability at each time.
11. Case Study: Probability of Network Packet Loss
Packet loss follows Bernoulli(p=0.02). Find probability of exactly 3 losses in 100 packets (Binomial).
12. Case Study: ARIMA Forecasting of CPU Load
Given 30 days of historical CPU usage, explain steps for ARIMA(1,0,1) fitting and forecasting 5 days.
13. Case Study: Markov Decision Process for Robot Navigation
Grid robot has 4 actions with transition probabilities. Formulate reward matrix and compute optimal policy conceptually.
14. Case Study: Logistic Regression for Disease Prediction
Dataset labels Stroke/No-Stroke. Explain how to compute odds ratio and interpret coefficients.
15. Case Study: Chi-Square Test for Website Click Patterns
Observed clicks on 3 sections: [120, 80, 100], Expected: [100,100,100]. Perform χ^2 test at 5% level.
16. Case Study: Probability of Cache Hit Ratio
Cache hit probability=0.75. For 20 requests, compute expected hits and variance (Binomial).

17. Case Study: Time Series Anomaly Detection (Z-Score Method)
Given data points, compute mean, SD, and flag values exceeding z>3 as anomalies.

Starting from 1st case study example every roll no has to solve one example .That is roll no-1 will solve first example ,roll no2 will solve 2nd example like this.

CA 2 Applications of Number Theory in Computation

Mode:- Print out

Total Marks:-10

Concept Understanding & Correct Implementation-4M, Problem

Solving & Analysis-3M,Presentation & Documentation-3M

Sr. No.	Roll No	Topic Name	Brief Description
1	1	Cryptography Using Modular Arithmetic	Basis of RSA, ElGamal, and secure communication.
2	2	Fast Modular Exponentiation	Speeds up encryption/decryption using binary exponentiation.
3	3	Prime Number Generation (Sieve Methods)	Sieve of Eratosthenes, Atkin for cryptographic primes.
4	4	Primality Testing Algorithms	Miller–Rabin, Fermat tests used in security systems.
5	5	Euclid & Extended Euclid Algorithm	Computes GCD and modular inverse for crypto.
6	6	Chinese Remainder Theorem (CRT)	Efficient large integer arithmetic & parallel computing.
7	7	Pseudorandom Number Generators (PRNG)	LCG, Blum-Blum-Shub for randomness in computing.
8	8	Elliptic Curve Cryptography (ECC)	Lightweight, secure cryptography for IoT and mobiles.
9	9	Error Detection & Correction Codes	CRC, Hamming codes, Reed–Solomon codes.
10	10	Modular Arithmetic in Hashing	Used in hash tables, bloom filters, load balancing.
11	11	Integer Factorization Algorithms	Pollard Rho, Fermat factorization used in breaking RSA.
12	12	Diophantine Equations in CS	Used in scheduling, crypto, coding theory.
13	13	Polynomial Arithmetic Over Finite Fields	AES encryption, RAID recovery, GF(2) operations.

Sr. No.	Roll No	Topic Name	Brief Description
14	**14**	Lattice-Based Cryptography	Post-quantum algorithms like NTRU.
15	**15**	Digital Signature Algorithms	RSA, DSA, ECDSA using number theory.
16	**16**	Randomized Algorithms Based on Number Theory	Monte Carlo & Las Vegas algorithms.
17	**17**	Modular Arithmetic in Computer Networks	Packet scheduling, checksum generation.

Yashoda Shikshan Prasarak Mandal's
YASHODA TECHNICAL CAMPUS, SATARA
FACULTY OF ENGINEERING
NH-4, Wadhe Phata, Satara., Tele Fax- 02162-271238/39/40
Website- www.yspmsatara.co.in Email-admin@yspmsatara.co.in
Approved by AICTE- New Delhi, Govt. of Maharashtra (DTE, Mumbai) Affiliated to DBATU Lonere.
DEPARTEMENT OF COMPUTER SCIENCE AND ENGINEERING

Starting from 1st case study example every roll no has to solve one example .That is roll no-1 will solve first example ,roll no2 will solve 2nd example like this.

CA 2 Applications of Number Theory in Computation

Mode:- Print out

Total Marks:-10

Concept Understanding & Correct Implementation-4M, Problem

Solving & Analysis-3M,Presentation & Documentation-3M

Sr. No.	Roll No	Topic Name	Brief Description
1	1	Cryptography Using Modular Arithmetic	Basis of RSA, ElGamal, and secure communication.
2	2	Fast Modular Exponentiation	Speeds up encryption/decryption using binary exponentiation.
3	3	Prime Number Generation (Sieve Methods)	Sieve of Eratosthenes, Atkin for cryptographic primes.
4	4	Primality Testing Algorithms	Miller–Rabin, Fermat tests used in security systems.
5	5	Euclid & Extended Euclid Algorithm	Computes GCD and modular inverse for crypto.
6	6	Chinese Remainder Theorem (CRT)	Efficient large integer arithmetic & parallel computing.
7	7	Pseudorandom Number Generators (PRNG)	LCG, Blum-Blum-Shub for randomness in computing.
8	8	Elliptic Curve Cryptography (ECC)	Lightweight, secure cryptography for IoT and mobiles.
9	9	Error Detection & Correction Codes	CRC, Hamming codes, Reed–Solomon codes.
10	10	Modular Arithmetic in Hashing	Used in hash tables, bloom filters, load balancing.
11	11	Integer Factorization Algorithms	Pollard Rho, Fermat factorization used in breaking RSA.
12	12	Diophantine Equations in CS	Used in scheduling, crypto, coding theory.
13	13	Polynomial Arithmetic Over Finite Fields	AES encryption, RAID recovery, GF(2) operations.
14	14	Lattice-Based Cryptography	Post-quantum algorithms like NTRU.

Sr. No.	Roll No	Topic Name	Brief Description
15	**15**	Digital Signature Algorithms	RSA, DSA, ECDSA using number theory.
16	**16**	Randomized Algorithms Based on Number Theory	Monte Carlo & Las Vegas algorithms.
17	**17**	Modular Arithmetic in Computer Networks	Packet scheduling, checksum generation.