Reg No.:_____ Name:_____

**APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY**

B.Tech Degree S6 (Minor) Examinations April 2026 (2023 Admn)

## Course Code: MAT382
## Course Name: ALGEBRA AND NUMBER THEORY

Max. Marks: 100 Duration: 3 Hours

### PART A

*Answer all questions, each carries 3 marks.* Marks

1 Suppose that $a \mid bc$, where $a, b, c \in \mathbb{Z}$ and $a$ and $b$ are relatively prime. Then prove that $a \mid c$. (3)

2 Compute $7^{13} \bmod 23$ using repeated squaring algorithm. (3)

3 Find $\phi(526)$ where $\phi$ is the Euler totient function. (3)

4 Determine the quadratic residues and non-residues modulo 13. (3)

5 Write the composition table for the finite group $(\mathbb{Z}_6, +_6)$. (3)

6 Find all the subgroups of $\mathbb{Z}/6\mathbb{Z}$ (3)

7 Find the generators of $\mathbb{Z}_{18}$ (3)

8 Find the order of the permutation $(1\ 6\ 2\ 3)(4\ 5)$ in $S_6$ (3)

9 Write down the units of $\mathbb{Z}/8\mathbb{Z}$ (3)

10 Prove that the ring of integers $\mathbb{Z}$ is a principal ideal domain. (3)

### PART B

*Answer one question from each module, each carries 14 marks.*

#### Module I

11 a) Use Euclidean algorithm to find integers $x$ and $y$ satisfying (7)

$$\gcd(252,198) = 252x + 198y$$

b) Solve the system of simultaneous congruences using the Chinese remainder theorem: (7)

$$x \equiv 1(\mathrm{mod}4), x \equiv 2(\mathrm{mod}5), x \equiv 3(\mathrm{mod}7)$$

**OR**

12 a) Let $m, n \in \mathbb{Z}$. Then prove that (7)
(i) $\gcd(m, 0) = m$ if $m \in \mathbb{N}$
(ii) $\gcd(m, n) = \gcd(m - qn, n)$ for every $q \in \mathbb{Z}$.

b) Suppose that $x_1 \equiv x_2 (\mathrm{mod}\ d)$ and $y_1 \equiv y_2 (\mathrm{mod}\ d)$, then prove that (7)

$$(x_1 + y_1) \equiv (x_2 + y_2) (\mathrm{mod}\ d)$$

#### Module II

13 a) Prove that every non-zero natural number $n$ is a product of prime numbers. (7)

b) Using RSA algorithm, if $p = 17, q = 11$ and $e = 7$, find the value of d and compute the cipher value of $q$ using the public key $(e, n)$. (7)

**OR**

14 a) Using Fermat's factorization method factorise $2^{11} - 1$. (7)

b) Prove that Let p be an odd prime. Then Prove that $-1$ is a quadratic residue modulo p if $p \equiv 1(\mathrm{mod}4)$ and a quadratic non-residue if $p \equiv 3(\mathrm{mod}4)$. (7)

**Module III**

15 a) Prove that If $H \subseteq G$ is a subgroup of a finite group G then $|G| = |G/H||H|$. i.e., the order of a subgroup divides the order of the group. (7)

b) Prove that a group has only one idempotent element (7)

**OR**

16 a) Check whether the map $f: (\mathbb{R}, +) \to (\mathbb{R}_{>0}, \cdot)$ where $\mathbb{R}_{>0} = \{x \in \mathbb{R} \mid x > 0\}$ by $f(x) = e^x$ is a group homomophism. (7)

b) Prove that $GL_2(\mathbb{R})$ is a non-abelian group. (7)

**Module IV**

17 a) Prove that a subgroup of a cyclic group is cyclic (7)

b) Consider $\mathbb{Z}_{12}$ with generator $a = 1$. Find the order of the cyclic subgroup generated by $5 \in \mathbb{Z}_{12}$ (7)

**OR**

18 a) Write $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix} \in S_6$ as a product of the minimal number of simple transpositions. (7)

b) Prove that every infinite cyclic group is isomorphic to $\mathbb{Z}$. (7)

**Module V**

19 a) Prove that every field is a domain. (7)

b) Prove that an ideal in a field F is either $\langle 0 \rangle$ or F itself. (7)

**OR**

20 a) Prove that every maximal ideal is a prime ideal. (7)

b) Prove that a ring homomorphism $f: R \to R$ is a one-one mapping if and only if $Ker\, f = \{0\}$. (7)

****