PreTest **Foundations of Computer Science** **Max:18 Marks**

Answer strictly within the space provided
Proper justification to your answers is **absolutely** necessary.

Name and Roll No.: ______________________________

1. In $\mathbf{Z_7^*}$, let S be the cyclic subgroup generated by 4. Write down the elements of the cosets $2S$ and $3S$. [3]

   Soln: $S = \{4, 4^2 \mod 7, 4^3 \mod 7\} = \{4, 2, 1\}$. $2S = \{8 \mod 7, 4 \mod 7, 2 \mod 7\} = \{1, 4, 2\} = S$. $3S = \{1.3 \mod 7, 4.3 \mod 7, 2.3 \mod 7\} = \{3, 5, 6\}$.

2. In the lattice $(\mathbf{Q}, \leq)$, What is $LUB(S)$ where $S = \{x | x^2 < 3\}$. What is $LUB(S)$ if the lattice is changed to $(\mathbf{R}, \leq)$? Justify your answer. [3]

   Soln: In $(\mathbf{Q}, \leq)$, $LUB(S)$ does not exist as there is no "smallest" rational number greater than $\sqrt{3}$. In $(\mathbf{R}, \leq)$, $LUB(S) = \sqrt{3}$.

3. In the group $\mathbf{Z_7^*} \times \mathbf{Z_3^*}$, what is the order of the element $(4, 2)$? Justify your answer. [3]

   Soln: By Question 1 above, $o(4) = 3$ in $\mathbf{Z_7}$. Since $2^2 = 1 \mod 3$, $o(2) = 2$ in $\mathbf{Z_3}$. Then, by Q.5 of Assignment 2, $o(4, 2) = LCM(3, 2) = 6$ in $\mathbf{Z_7^*} \times \mathbf{Z_3^*}$

4. In the group $(\mathbf{R}^2, +)$, consider the subgroup S consisting of all points on the line $y = 0$. Find the equation to the line defining $(1, 2) + S$. What is the equation to the line defining the sum of the cosets $(1, 2) + S$ and $(3, 4) + S$? [3]

   Soln: $y = 0$ is the x axis. Shifting this line with $(1, 2)$ yields the line $y = 2$ which is $(1, 2) + S$. By Q.6 and Q.7 of Assignment 2, $[(1, 2) + S] + [(3, 4) + S] = ((1, 2) + (3, 4)) + S = (4, 6) + S$. Shifting $y = 0$ by $(4, 6)$ yields the line $y = 6$.

5. For how many values of $a \in \{1, 2, 3, ..., 499\}$ it must be true that $a^{200} \neq 1 \mod 500$? Justify your answer. [3]

   Soln: It is not hard to see (by Euclid's algorithm and Euler's theorem) that $a^{\phi(n)} = 1 \mod n$ if and only if $GCD(a, n) = 1$ for all n. Thus all $1 \leq a \leq 499$ with $GCD(500, 1) \neq 1$ will satisfy $a^{\phi(500)} = a^{200} \neq 1 \mod 500$. There must be $499 - \phi(500) = 299$ such elements

6. In the group $\mathbf{Z}$, consider the smallest subgroup S containing both the elements 12 and 9. Prove that S is cyclic. Find at least two cyclic generators for S. (Use reverse side). [3]

   Soln: Clearly since $12, 9 \in S$, $12 - 9 = 3 \in S$. Consequently, all multiples of 3 must be in S. It is not hard to see that S is indeed all multiples of 3. Thus $S = 3\mathbf{Z}$. Note that 3 and -3 are generators for this group.

   In general, if a subgroup S of $\mathbf{Z}$ is generated by a and b, by definition of a group, all numbers of the form $\{ax + by : x, y \in \mathbf{Z}\}$ must be in S. This is precisely the group generated by $GCD(a, b)$. Both $GCD(a, b)$ and $-GCD(a, b)$ are generators for this group.