

-
- Kindly read and understand the preview of your end sem paper.
 - These questions will carry 20 marks.
 - An additional 20 marks will be based on other topics.
-

1. The labelled tree corresponding to a Pratt certificate for primality of a prime number $p \geq 2$ (when $p = 2$, the tree will contain just a single node labeled 2) can be constructed as follows.

5

- Let $p_1^{e_1} \times p_2^{e_2} \times \dots \times p_k^{e_k}$ be a prime factorization of $p - 1$.
- Let T_{p_i} be the labelled tree corresponding to a Pratt certificate of p_i .
- The root node of a Pratt certificate will be labelled by a generator for \mathbb{Z}_p^* .
- Each pair (p_i, e_i) will be a child of the root node. The child nodes with label (p_i, e_i) will have T_{p_i} as its child.

2. Consider the set of predicate logic formulae with a single function symbol $+$ and a single predicate symbol $<$. The interpretations we consider will have the underlying set \mathcal{Z} and $+$ will be interpreted as integer addition and $<$ will be interpreted as *less than* on integers. Find out an interpretation which makes the following formulae true.

5

3. A binary relation on any set X is a subset of $X \times X$. Let $S \subseteq \mathbb{R}$. Consider a binary relation E on \mathcal{R} defined as $\{(x, y) | x - y \in S\}$.

5

4. Consider a graph G . We want to label all the edges with bit strings of length k . While labelling it is desired that the labellings of adjacent vertices differ in exactly one position. Also every vertex should have a distinct label. We say that a graph is “encodable” if we can label it in such a way that for every pair of vertices u, v , the distance from u to v is same as the number of positions in which the labels of u and v differ.

5

* * *