Discrete Structures

IIIT Hyderabad

Monsoon 2020

Tutorial 5

September 30, 2020

Introduction

1. Questions
   - Question 0
   - Question 1
   - Question 2

Question 0

0.1: Prove that if R, S are transitive $\implies$ $R \cap S$ is transitive.

Sol: Let's assume it isn't.

$$\begin{aligned}
&(a,b) \in R \cap S) \wedge ((b,c) \in R \cap S) \wedge ((a,c) \notin (R \cap S)) \\
&\implies (((a,b) \in R) \wedge ((b,c) \in R) \wedge ((a,b) \in S) \wedge ((b,c) \in S)) \\
&\implies ((a,c) \in R) \wedge ((a,c) \in S) \\
&\implies (a,c) \in (R \cap S)
\end{aligned}$$

This is a contradiction and hence we say our assumption is wrong.

0.2: Let R be a reflexive relation on set A. Show that R is an equivalence relation if and only if (a, b) and (a, c) are in R implies that (b, c) is in R.
Sol: Since the solution is **if and only if** we have to prove the implications both ways.
LHS: Here we assume that the LHS is true and show that the *RHS* is also true.
Since R is an equivalence relation, $(a, b) \in R \implies (b, a) \in R$ (symmetric), and then $(b, a), (a, c) \in R \implies (b, c) \in R$ (transitive). Thus *RHS* is proved.
RHS: Here we assume that *RHS* is true and show that *LHS* is also true.
Since R is reflexive $(a, a) \in R$, then $(a, b), (a, a) \in R \implies (b, a) \in R$, thus R is symmetric.
Now for transitive case, we are given $(a, b), (b, c) \in R$ we have to show $(a, c) \in R$. Since $(a, b) \in R \implies (b, a) \in R$ as R is symmetric, then using the given relation $(b, a), (b, c) \in R \implies (a, c) \in R$. Thus R is also transitive. Thus R is an equivalence set.

Question 1

INTERNATIONAL INSTITUTE OF INFORMATION TECHNOLOGY HYDERABAD

1.1: Find $\phi(120)$.

Sol: $120 = 2^3 \cdot 3 \cdot 5$. It is equal to $2 \cdot 4 = 8$.

1.2: Find a number $a < p$ such that $a \cdot p = 1 \bmod(p)$ (modular inverse) without using any online tools. $(p = 13, a = 4)$.

Sol:

[Hint: Use Extended Euclid's Division Algorithm]

$$
\begin{aligned}
31 &= 12x2 + 7 \\
12 &= 7x1 + 5 \\
7 &= 5x1 + 2 \\
5 &= 2x2 + 1 \\
1 &= 5 - 2x2 \\
1 &= (12 - 7) - 2x(7 - (12 - 7)) \\
1 &= (12 - 7) - 2x(2x7 - 12) \\
1 &= (12 - (31 - 12x2)) - 2x(2x(31 - 12 * 2) - 12) \\
1 &= 13x12 - 5x31
\end{aligned}
$$

Thus we have 13 as module inverse.

Question 2

An encoding scheme is defined as follows -
A = 00, B = 01, C = 02 and so on, and 00 for space. Take $p = 13, q = 17$ and the public key (e) as 5.

1. Find the private key.
   Sol: $n = p \times q = 221$. We have $\phi(n) = 12 \times 16 = 192$. The private key ($d$) is, $5^{-1} (\text{mod } \phi(n))$. We use extended algorithm -

$$\begin{aligned} 192 &= 38 \times 5 + 2 \\ 5 &= 2 \times 2 + 1 \\ 1 &= 5 - 2 \times 2 \\ 1 &= 5 - 2 \times (192 - 38 \times 5) \\ 1 &= 77 \times 5 - 2 \times 192 \end{aligned}$$

   Thus, we get out private key as 77.

2. Find the ciphertext of the message "HI ALL". We will first encode the message "HI ALL", which encodes to 07 08 26 00 11 11. Now let us use chunk size of 1 letter -

$$07^5 \bmod (221) = 11$$
$$08^5 \bmod (221) = 60$$
$$26^5 \bmod (221) = 195$$
$$11^5 \bmod (221) = 163$$
$$11^5 \bmod (221) = 163$$

Thus our ciphertext is 11 60 195 163 163.

2. Decrypt the ciphertext to verify the same.

We use the private key $d = 77$, now -

$$11^{77} \text{mod } (221) = 07$$
$$60^{77} \text{mod } (221) = 08$$
$$195^{77} \text{mod } (221) = 26$$
$$163^{77} \text{mod } (221) = 11$$
$$163^{77} \text{mod } (221) = 11$$

Thus we get our decrypted ciphertext as 07 08 26 11 11. We decode it as "HI ALL" to get our message back.