CS201A : Mathematics for CS - I (Discrete Mathematics)
Assignment 1 Solution

Que (1) Let p be a prime number.

(a) Show that if m^2 is divisible by p then m is divisible by p.

Proof by contraposition
Let A : m^2 is divisible by p
Let B : m is divisible by p
To prove, $A \rightarrow B$, we will prove $\neg B \rightarrow \neg A$
$\neg B$: m is not divisible by p
By prime factorization theorem,
m = $m_1^{a_1} \times m_2^{a_2} \times m_3^{a_3} \times .... \times m_k^{a_k}$ where $m_i \in \mathcal{N} \setminus \{1, p\}$ are primes and $a_i \in \mathcal{N}$
$\Rightarrow m^2 = m_1^{2a_1} \times m_2^{2a_2} \times m_3^{2a_3} \times .... \times m_k^{2a_k}$
Here, $m_i \neq p$ $\forall i \in \{1, 2, 3, ..., k\}$ and m_i are primes. We have got a prime factoriztion of m^2 which does not contain p as one of the prime factors.
Hence, we can say that m^2 is not divisible by p.
We proved, $\neg B \rightarrow \neg A$ which is equal to proving $A \rightarrow B$.

(b) Will (a) hold if p is composite? Prove your answer.

No (a) will not hold if p is composite.
A counter example for it :
Let m = 2, p = 4
Here, p divides m^2 but it does not divide m.

(c) Using (a) prove that $\sqrt{p}$ is always irrational.

Proof by contradiction
Assume that $\sqrt{p}$ is rational and
$\sqrt{p} = \frac{a}{b}$ where a and b are coprimes.
$\Rightarrow$ p = $\frac{a^2}{b^2}$
$\Rightarrow b^2 = \frac{a^2}{p}$ ...... (1)
$\Rightarrow$ p | a^2
$\Rightarrow$ p | a (from (a)) ...... (2)
Since, p | a, let a = p × k (k ∈ $\mathcal{Z}$)
Substituting in (1),
$b^2 = \frac{p^2k^2}{p}$
$\Rightarrow b^2$ = p k^2
$\Rightarrow$ p | b^2 (as k^2 is an integer)
$\Rightarrow$ p | b (from (a)) ...... (3)
From (2) and (3), we can say that p is a common factor in a and b.
But that is contradictory as we have assumed a and b as coprimes.
Hence, our assumption is wrong.
$\Rightarrow \sqrt{p}$ is always irrational.

Que (2)

(a) Show that if real number x satisfies the equation:
$x^n + c_1x^{n-1} + ... + c_{n-1}x + c_n = 0$
where c_i i = 1...n are integers then x is either an integer or an irrational number.

Proof by contradiction
Let x $\in \mathcal{Q} \setminus \mathcal{Z}$, x = $\frac{a}{b}$ where a, b $\in \mathcal{Z}$, a and b are coprimes, b $\neq$ 0, 1, -1
Substituting x in above equation,
$\left(\frac{a}{b}\right)^n + c_1 \left(\frac{a}{b}\right)^{n-1} + ... + c_{n-1}\left(\frac{a}{b}\right) + c_n = 0$
$\Rightarrow a^n + c_1ba^{n-1} + ... + c_{n-1}ab^{n-1} + c_nb^n = 0$
$\Rightarrow a^n$ = - b ($c_1a^{n-1} + c_2a^{n-2}b + ... + c_nb^{n-1}$)
$\Rightarrow$ b | a^n (as c_i, a, b are integers)
$\Rightarrow$ b | a^{n-1} (because a and b are coprimes)
$\Rightarrow$ b | a (by appying above argument)
$\Rightarrow$ b = 0, -1, 1 (as a and b are coprimes)
But that is contradictory.
Hence, x $\notin \mathcal{Q} \setminus \mathcal{Z}$
$\Rightarrow$ x is either an integer or an irrational number.

(b) Use (a) above to argue that if positive integer m is not equal to the n^{th} power of some integer then $\sqrt[n]{x}$ is irrational.

Substituting c_i = 0 and c_n = -m in equation of (a), we get
$\Rightarrow x^n$ - m = 0 where n, m $\in \mathcal{N}$
From (a), we can say that above equation has either integer or irrational roots.
But is is given that, m $\neq k^n$, k $\in \mathcal{Z}$
Hence, x can not be an integer.
$\Rightarrow$ x is irrational.
$\Rightarrow$ x = $\sqrt[n]{m}$ is irrational.

(c) Argue that if $\sqrt{n}$ is irrational and $\sqrt{n} = \sqrt{ab}$ then $\sqrt{a} + \sqrt{b}$ is irrational.
[To prove this, we will assume a, b $\in \mathcal{Q}$]

Let, $\sqrt{a} + \sqrt{b}$ be rational.
$\Rightarrow \sqrt{a} + \sqrt{b} \in \mathcal{Q}$
$\Rightarrow$ a + b + 2 $\sqrt{ab} \in \mathcal{Q}$ (Squaring both the sides)
$\Rightarrow$ a + b + 2 $\sqrt{n} \in \mathcal{Q}$
$\Rightarrow \sqrt{n} \in \mathcal{Q}$ (Since a and b are rational.)
which is contradictory.
Hence, $\sqrt{a} + \sqrt{b}$ is irrational.

[If a, b $\in \mathcal{R}$ then the given statement is wrong which can be seen by taking
a = $(2+\sqrt{6})^2$ and b = $(3-\sqrt{6})^2$]

Que (3)

(a) Let $S_0 = 0$, $S_1 = 1$ for n $\in \mathcal{N}$, n >1 S_n = 5S_{n-1} - 6S_{n-2} Show by induction that $S_n = 3^n$ - 2^n .

Proof:
Basis: S_0 = 0 and S_1=1 (given)
S_0=3^0-2^0=0

S_1=3^1-2^1=1
Induction: Assume it is true $\forall$ k$\leq$n.
so,
S_{n-1}=3^{n-1}-2^{n-1}
S_n=3^n-2^n
To prove:this is true for n+1 ie
S_{n+1}=3^{n+1}-2^{n+1}

As we know ,
S_n = $5S_{n-1}$ - $6S_{n-2}$, $\forall$ n $\in$ N, n >1
So, from inductive step, we take the values for
S_n and S_{n-1}

S_{n+1} = 5(3^n-2^n) - 6(3^{n-1}-2^{n-1})
= 3^{n-1}(5*3-6)-2^{n+1}(5*2-6)
= 3^{n-1}*9 -2^{n-1} * 4
= 3^{n+1}-2^{n+1}
Hence, it is true for K = n+1, or we can say $\forall$ n $\in$ N and n >1

(b) $\forall$ n $\in$ N
1$\times$2 + 2$\times$ 3 + ... + (n-1)$\times$n = $\frac{(n-1)n(n+1)}{3}$

Basis: For n=1,

LHS: $\frac{(n-1)n(n+1)}{3} \Rightarrow 0 \times 1 = 0$

RHS: $\frac{(n-1)(n)(n+1)}{3}$

$\Rightarrow \frac{0.1.2}{3} = 0$

$\Rightarrow$ LHS=RHS

Induction: Assume it is true for $\forall$ k $\leq$ n,
for k = n, 1$\times$2 + 2$\times$ 3 + ... + (n-1)$\times$n = $\frac{(n-1)n(n+1)}{3}$
To prove: it is true for k = (n+1).
LHS: 1 $\times$ 2 + 2 $\times$ 3 + ...+ (n-1)$\times$n + n$\times$(n+1)
As we know, 1$\times$2 + 2$\times$ 3 + ... + (n-1)$\times$n = $\frac{(n-1)n(n+1)}{3}$
so,putting it in above equation, we get

$\frac{(n-1)n(n+1)}{3}$ + n$\times$(n+1) = $\frac{(n+1)n(n-1+3)}{3}$
$\frac{n(n+1)(n+2)}{3}$ = RHS
So, it is true $\forall$ n $\geq$ 0.

(c) Prove that the number of subsets of a set with n elements, n $\geq$ 0 is 2^n.

Basis:- As empty set is a set itself so, having zero elements has 2^0 subsets.
Induction:- Assume every n-element set has 2^n subsets.
To Prove:- Every (n+1)-element set has 2^{n+1} subsets.
Let A=$\{a_1, a_2, ..., a_n, a_{(n+1)}\}$ having (n+1) elements. We partition power set of A$\Big(P(A)\Big)$ into two subset sets $say\Big(P_1(A)\&P_2(A)\Big)$, where $P_1(A)$ contains subsets of A which don't have $a_{(n+1)}$ in them and the $P_2(A)$ contains subsets of A which have $a_{(n+1)}$ in them.
So, $P_1(A)$ is made up of all subsets from n element set $\{a_1, a_2, ..., a_n\}$ so it has 2^n subsets.

Now, by construction, it follows that the second power set i.e., $P_2(A)$ must have same number of enteries as the powerset $P_1(A)$, so it too has 2^n subsets.

Since, union of $P_1(A)$ and $P_2(A)$ leads to the $P(A)$ so we see that
So, Power Set of A has 2^{n+1} elements (or subsets) in it.
Hence Proved.

(d) Show that the number of permutations of a string of n letters is n!

Basis:- For n=1, one letter can have 1 permutation
1 ! = 1
So, it is true for n=1
Induction:- Let it is true for n letters.
So, Number of permutation of n letters is n!.
To Prove:- for (n+1) letters it is (n+1)!
Consider one of the permutations of n letters. We have (n+1) positions to insert a new letter in it. By inserting a new letter at every position, we will get a new permutation of (n+1) letters.
we know that
No. of permutations of a string of n letters is n!.
So, total permutations of (n+1) letters is (n+1) n! = (n+1)! .

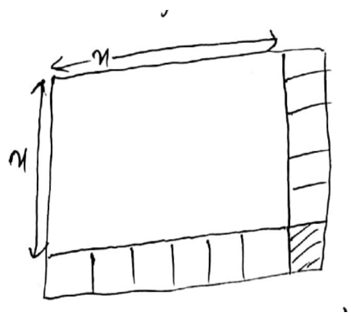
Que (4) Consider the following colouring problem. We are given an $n \times n$ board of white squares where some $m < n^2$ randomly chosen squares are coloured red. In each round some more white squares are coloured red according to the following two rules:
a) already red squares remain red,
b) a white square that has at least 2 red neighbours is coloured red where a neighbour is defined as those squares that are immediately to the left/right/up/down (that is LRUD neighbours) of the white square.
Intuitively, it is clear that if enough squares are initially red then in finitely many rounds the whole board will be coloured red.
Formulate a conjecture on a necessary lower bound for m (the number of initially coloured red squares) such that it is possible the whole board is coloured red after finitely many rounds. Prove your conjecture.
For example, if we have a 3×3 board and only 2 squares are coloured red the whole board can never be coloured red.

Solution:
It can be observed that if we color any one of the main diagonals of $n \times n$ board, After finite rounds whole board can be colored red.
Conjecture: Minimum number of initially red coloured squares s.t it is possible to color whole $n \times n$ board red after finite rounds is n.
To prove the conjecture we need to prove these two prepositions:

1. There exists a way to color $n \times n$ board red given that initially n squares are colored red.

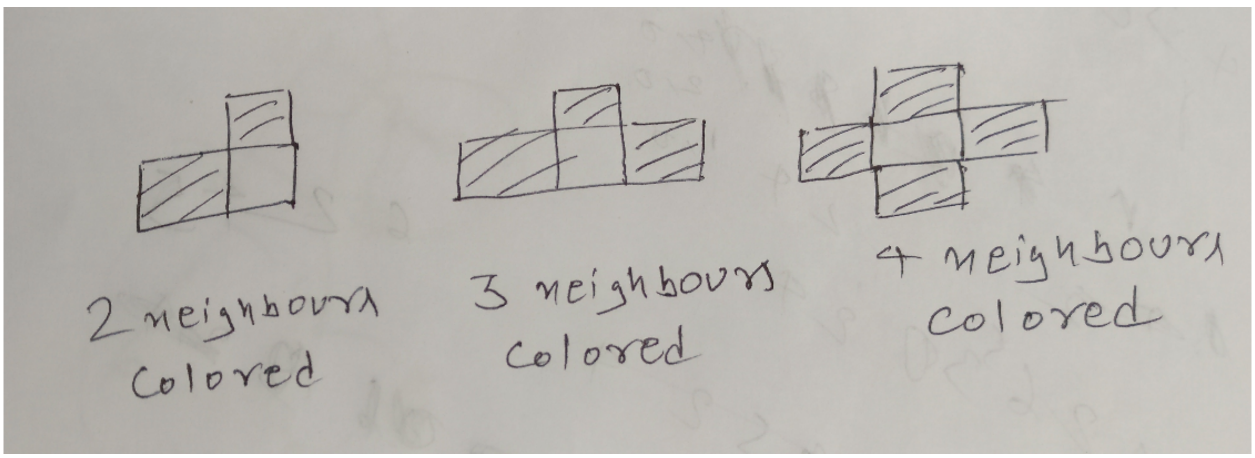
2. It is not possible to color $n \times n$ board red given that initially m squares are colored red s.t $m < n$.

Proof for 1:
Base Case: when n=1 , board has one square, coloring which makes the whole board red.
Induction step: Let n initially colored red squares can make the board colored red in finite steps.
Then for board of size $(n+1) \times (n+1)$, we have one row and one column left uncolored.



If we color the square at the intersection of this row and column as shown, In subsequent steps both the row and column can be colored red completely which completes the coloring of whole $(n+1) \times (n+1)$ board.
Conclusion: By principle of induction, we have proved that prep.1 holds for all $n \in \mathbb{N}$.

Proof for 2:
There are only 3 cases in which a new square can be colored red using the rules given in question.



Consider the boundary of red colored region, In all cases either the length of boundary remains same or decreases.
For fully red colored board, boundary length $= 4 \times n$.
If we consider m initially red colored squares s.t $m < n$, max. length of boundary $= 4 \times (n-1)$.
$\because 4 \times (n-1) < 4 \times n$ and boundary length can never increase with given coloring rules
$\therefore$ It is not possible to color $n \times n$ board red with initially m red colored squares s.t $m < n$.
Proving prep.1 and prep.2 proves the conjecture.

Que (5)

(a) For the base case, taking n = 1, 1(1+1) = 2, we get an even number. Hence, the claim does not hold for the base case. We need the base case true for applying the principle of mathematical induction. The given proof is incorrect.

(b)

Int the induction hypothesis, it is assumed that if there are n-1 lines in the plane, no two of which are parallel, then they all go through one point. We have sets S, $S^{'}$ and S'' in the proof. Set S is a set of n lines, no two of which are parallel. Sets $S^{'}$ and S'' are of n-1 lines and their single point of intersections $P^{'}$ and $P^{''}$ respectively. The proof takes $P^{'}$ and $P^{''}$ be to same but our hypothesis doesn't claim that all set of n-1 lines will have a common point of intersection. Therefore, the induction step for a set of size n is wrong. The given proof is incorrect.

(c) In the proof, it is assumed that the claim is true for n and n-1. So, along with n=0, we need to include n=1 for the base case. But for the base case n=1, the claim does not hold. Hence, induction hypothesis assumption is wrong and the given proof is incorrect.