Final Examination -- Solution

Instructions:

- Return the question paper together with the answer script. Read each question completely before answering it. There are **7 questions and 4 pages.** Each question consists of **5 parts.**
- In case of any ambiguity, you may make assumption. But your assumption should not contradict any statement in the question paper.
- For the problems below, we can award partial credit only if you show your work.
- Attempt all the questions (parts) in the given sequence of the question paper.

Total Time: 3 Hours **Maximum Points**: 70 Points

Question # 1: Propositional Logic, Rules of Inference, Predicate Logic and Quantifiers [2x5 =10 points]

(i) Consider the following system specifications using the given propositions:

P = "The message is scanned for viruses." **Q =** "The message was sent from an unknown system."

(a) The message is scanned for viruses whenever the message was sent from an unknown system. $Q \rightarrow \boldsymbol{P}$

(b) The message was sent from an unknown system but it was not scanned for viruses. $Q \wedge \neg \boldsymbol{P}$

(c) When a message is not sent from an unknown system, it is not scanned for viruses. $\neg Q \rightarrow \neg \boldsymbol{P}$

(ii) Determine using laws of logic if the given expression is a tautology, contradiction or a contingency.

$$\big((\boldsymbol{x} \vee \boldsymbol{y}) \wedge (\boldsymbol{x} \rightarrow \boldsymbol{z})\big) \rightarrow (\boldsymbol{y} \vee \boldsymbol{z})$$

Solution:

$\equiv \big((x \vee y) \wedge (x \rightarrow z)\big) \rightarrow (y \vee z)$	
$\equiv \neg\big((x \vee y) \wedge (\neg x \vee z)\big) \vee (y \vee z)$	Implication Law
$\equiv \big(\neg(x \vee y) \vee \neg(\neg x \vee z)\big) \vee (y \vee z)$	De-Morgan Law
$\equiv \big((\neg x \wedge \neg y) \vee (\neg\neg x \wedge \neg z)\big) \vee (y \vee z)$	De-Morgan Law
$\equiv \big((\neg x \wedge \neg y) \vee (x \wedge \neg z)\big) \vee (y \vee z)$	Double Negation
$\equiv (\neg x \wedge \neg y) \vee y \vee (x \wedge \neg z) \vee z$	Associative and commutative law
$\equiv ((\neg x \vee y) \wedge (\neg y \vee y)) \vee ((x \vee z) \wedge (\neg z \vee z))$	Distributive Law
$\equiv ((\neg x \vee y) \wedge T) \vee ((x \vee z) \wedge T)$	Negation Law
$\equiv (\neg x \vee y) \vee (x \vee z)$	Identity Law
$\equiv (\neg x \vee x) \vee (y \vee z)$	Associative and commutative law
$\equiv T \vee (y \vee z)$	Negation Law
$\equiv T$	Domination Law

Hence it's a tautology.

(iii) Using Rules of inference, show that the following argument is valid.

((¬b → (c → ¬d)) ∧ (¬b ∨ f) ∧ (¬a → c) ∧ (¬f)) → (d → a)

Solution:

$= \underline{((\neg b \vee f) \wedge (\neg f)} \wedge (\neg b \rightarrow (c \rightarrow \neg d)) \wedge (\neg a \rightarrow c))$	*Disjunctive Syllogism*
$= \underline{((\neg b) \wedge (\neg b \rightarrow (c \rightarrow \neg d)) \wedge} (\neg a \rightarrow c))$	*Modus Ponens*
$= \underline{(\neg a \rightarrow c) \wedge (c \rightarrow \neg d)}$	Hypothetical Syllogism
$= \underline{(\neg a \rightarrow \neg d)}$	Contrapositive
$= d \rightarrow a$	

(iv) Suppose P (x, y) is the predicate **"x has taken y,"** the domain for x consists of all pupil in this class, and the domain for y consists of all Discrete Structure lectures. Write the following predicate expressions in good English without using variables in your answers:

(a) $\exists x \exists y\, P(x, y)$

Solution: "There is a pupil in this class who has taken a Discrete Structures Lecture."
(b) $\neg\forall y\ \forall x\ P(x, y)$
Solution: "Not all Discrete Structures Lectures have been taken by all pupils in this class."

(v) Write the predicate expressions of the following statements using variables and any needed quantifiers:
(a) "The product of two negative real numbers is not negative."
Solution: $\forall x\ \forall y\ ((x < 0) \wedge (y < 0) \rightarrow (xy > 0))$
(b) "The difference of a real number and itself is zero."
Solution: $\forall x(x - x = 0)$

QUESTION # 2: Set Theory, Relations and Functions **[2x5 =10 points]**

(i) Let ***X*** and ***Y*** be two sets. Prove or disprove using the set builder notation that ***A U (B − A) = A U B.***
Solution:

$$
\begin{aligned}
& x \in A \cup (B - A) \\
\Longleftrightarrow \quad & x \in A \vee x \in (B - A) \\
\Longleftrightarrow \quad & x \in A \vee (x \in B \wedge x \notin A) \\
\Longleftrightarrow \quad & (x \in A \vee x \in B) \wedge (x \in A \vee x \notin A) \\
\Longleftrightarrow \quad & x \in A \vee x \in B \\
\Longleftrightarrow \quad & x \in A \cup B
\end{aligned}
$$

Thus, $A \cup (B - A)$ and $A \cup B$ have the same elements, so they're equal.

(ii) Suppose in sets A, B, & C, the set $B \cap C$ consists of 8 elements, set $A \cap B$ consists of 7 elements and set $C \cap A$ consists of 7 elements then how many minimum elements will be there in set **A U B U C**?
Solution:
There would be 8 elements in set A U B U C.
As minimum elements set B and C have 8 elements each and all of the elements are same, also set A should have 7 elements which are already present in B and C. Thus, A U B U C ≡ A ≡ B.

(iii) A tournament graph G = (V, E) is a directed graph such that there is either an edge from a to b or an edge from b to a for every distinct pair of nodes a and b. (The nodes represent players and an edge $a \rightarrow b$ indicates that player a beats player b.) Consider the "beats" relation implied by a tournament graph. Indicate whether Partial order or Equivalence relation hold for all tournament graphs and briefly explain your reasoning. You may assume that a player never plays herself.
Solution: For Equivalence relation, we have to check Reflexive, Symmetric and Transitive property whereas for partial order relation we have to check Reflexive, Antisymmetric and Transitive property.
1. Reflexive: The "beats" relation is not reflexive since a tournament graph has no self-loops.
2. Symmetric: The "beats" relation is not symmetric by the definition of a tournament: if x beats y then y does not beat x.
3. Antisymmetric: The "beats" relation is antisymmetric since for any distinct players x and y, if x beats y then y does not beat x.
4. Transitive: The "beats" relation is not transitive because there could exist a cycle of length 3 where x beats y, y beats z and z beats x. By the definition of a tournament, x cannot then beat y in such a situation.
Hence, beat relation is neither equivalence nor partial order relation.

(iv) Let $f: \mathbb{R} \rightarrow \mathbb{R}$ be defined by the formula $f(x) = 4x\text{-}1;\ \forall x \in R.$ Is ***f*** a bijective function? If no, give reason why? If yes, find its inverse.
Solution:

Then f is bijective, therefore f^{-1} exists. By definition of f^{-1},

$f^{-1}(y) = x \Leftrightarrow f(x)=y$

Now solving $f(x) = y$ for x

$\Leftrightarrow$ $4x-1 = y$ (by definition of f)

$\Leftrightarrow$ $4x = y + 1$

$\Leftrightarrow$ $x = \dfrac{y+1}{4}$

Figure # 2

Hence, $f^{-1}(y) = \dfrac{y+1}{4}$ is the inverse of $f(x)=4x-1$ which defines $f^{-1}: R \to R$.

(v) Prove or disprove the statement $\lceil m + n \rceil = \lceil m \rceil + \lceil n \rceil$ for real numbers m and n.

Solution:

Acounterexample: $m = 1/2$ and $n = 1/2$

LHS: $\lceil m + n \rceil = \lceil 1/2+1/2 \rceil = \lceil 1 \rceil = 1$

RHS: $\lceil m \rceil + \lceil n \rceil = \lceil 1/2 \rceil + \lceil 1/2 \rceil = 1+1 = 2$

It is false

<u>Question # 3: Graph Theory</u> **[2x5=10points]**

Musab is an undergraduate student. The following graph map (Figure # 1) shows different path from his home to the school.

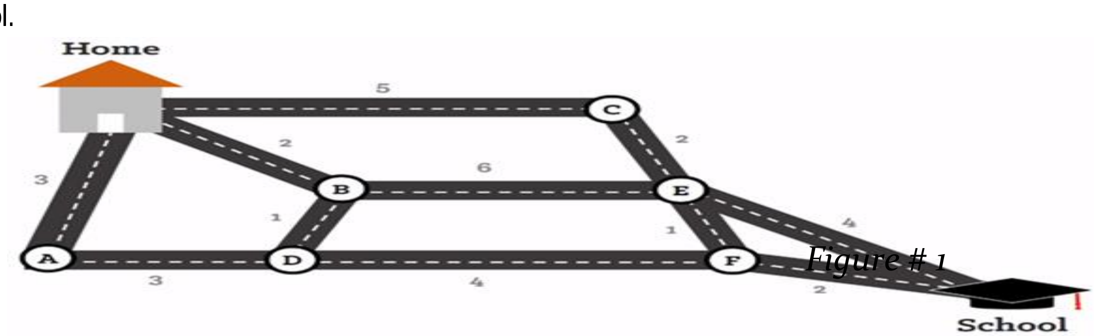


Figure # 1

(i) Musab wants to determine the shortest path from home to school using Dijkstra Algorithm. What will be the cost of that path? Show all steps.

Solution:

The shortest path, which could be found using Dijkstra's algorithm, is Home →B→D→F→ School

Cost: 2 + 1 + 4 + 2 = 9.

N	D(A)	D(B)	D(C)	D(D)	D(E)	D(F)	D(S)
H	3,H	2,H	5,H	∞	∞	∞	∞
HB	3,H		5,H	3,B	8,B	∞	∞
HBA			5,H	3,B	8,B	∞	∞
HBAD			5,H		8,B	7,D	∞
HBADC					7,C	7,D	∞
HBADCE						7,D	11,E
HBADCEF							9,F
HBADCEFS							

(ii) Determine the Euler Circuit and Path in the above graph for Musab? Show all of your steps with reasoning.

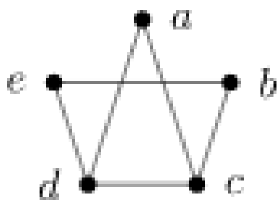
Solution:

No Euler Circuit possible because some nodes have odd vertices. No Euler path is possible because there are more than two vertices with odd degree.

(iii) Determine the Hamilton Circuit and Path in the above graph for Musab? Show all of your steps with reasoning.
Solution:
No Hamilton Circuit But path is possible. E.g: C-> E-> S -> F-> D-> B-> H-> A

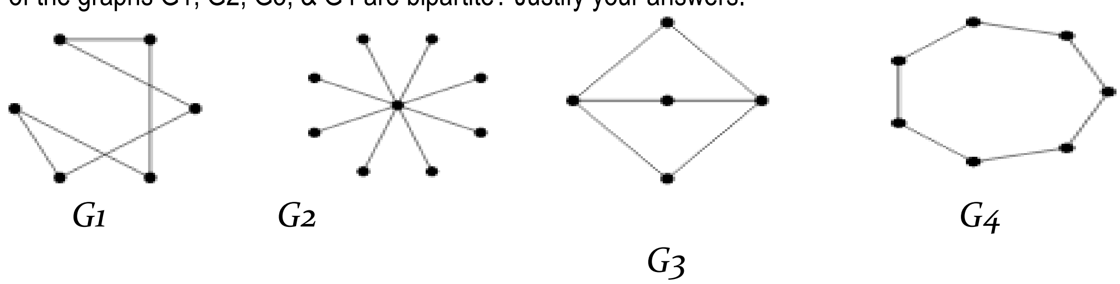
(iv) Determine if the following two graphs Graph #1 and Graph #2 are Isomorphic. If they are, give function F: V(G1) ⟶ V(G2) that define the Isomorphism. If they are not, give the reason why?
Graph 1: V = {a, b, c, d, e}, E = {{a, b}, {a, c}, {a, e}, {b, d}, {b, e}, {c, d}}.

Graph 2:



Solution:
F: G1⟶G2 defined by f(a)=d, f(b)=c, f(c)=e, f(d)=b, f(e)=a.

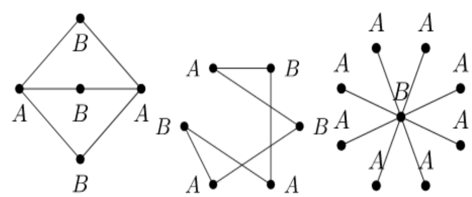
(v) Which of the graphs G1, G2, G3, & G4 are bipartite? Justify your answers.



Solution:

Answer

Three of the graphs are bipartite. The one which is not is C_7 (second from the right). To see that the three graphs are bipartite, we can just give the bipartition into two sets A and B, as labeled below:



The graph C_7 is not bipartite because it is an *odd* cycle. You would want to put every other vertex into the set A, but if you travel clockwise in this fashion, the last vertex will also be put into the set A, leaving two A vertices adjacent (which makes it not a bipartition).

Question # 4: Sequence & Series and Trees **[2x5=10 points]**

(i) Consider the function f: N⟶N given by f(0)=0 and f(n+1)=f(n)+2n+1. Find f (6).
Solution:

The rule says that $f(6) = f(5) + 11$ (we are using $6 = n + 1$ so $n = 5$). We don't know what $f(5)$ is though. Well, we know that $f(5) = f(4) + 9$. So we need to compute $f(4)$, which will require knowing $f(3)$, which will require $f(2)$,... will it ever end?

Yes! In fact, this process will always end because we have $\mathbb{N}$ as our domain, so there is a least element. And we gave the value of $f(0)$ explicitly, so we are good. In fact, we might decide to work up to $f(6)$ instead of working down from $f(6)$:

$$\begin{aligned}
f(1) &= f(0) + 1 = & 0 + 1 &= 1\\
f(2) &= f(1) + 3 = & 1 + 3 &= 4\\
f(3) &= f(2) + 5 = & 4 + 5 &= 9\\
f(4) &= f(3) + 7 = & 9 + 7 &= 16\\
f(5) &= f(4) + 9 = & 16 + 9 &= 25\\
f(6) &= f(5) + 11 = & 25 + 11 &= 36
\end{aligned}$$

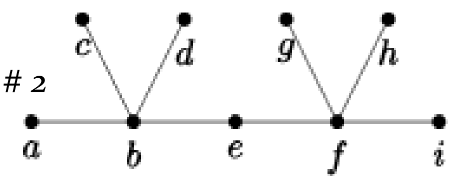
(ii) Express in sigma notation the sum of the first 50 terms of the series 2 + 4 + 6 + 8 + 10 + 12 +. ...

Solution:

In sigma notation we have $\sum_{i=1}^{50} 2i$. Note that we could also write this in other forms, for example $\sum_{j=1}^{50} 2j$ or $\sum_{k=1}^{50} 2k$ (we can use any variable as the index of summation). We can also change the limits of summation, obtaining forms such as the sum $\sum_{i=0}^{49} 2(i+1)$.

(iii) Construct Pre-order, Post-order and In-order traversals of the given tree(rooted at e) as shown in Figure # 2.

Figure # 2



Solution:

Pre-order: e, b, a, c, d, f, g, h, i

Post-order: a, c, d, b, g, h, i, f, e

In-order: a, b, c, d, e, f ,g, h, i

(iv) Construct the Minimum Spanning Tree (MST) for the given graph in Figure # 3 using PRIM'S and KRUSKAL'S algorithms.

Solution:

Prims Algorithm: Order of edges added: (a, b) = 3, (b, c) =2, (c, d) = 1, (c, e) =4, (e, f) =3.

Kruskal's algorithm: Order of edges added: (c, d) = 1, (b, c) =2, (a, b) = 3, (e, f) =3, (c, e) =4.

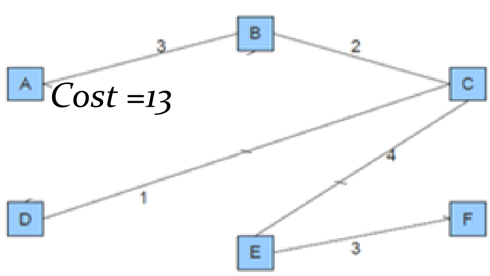
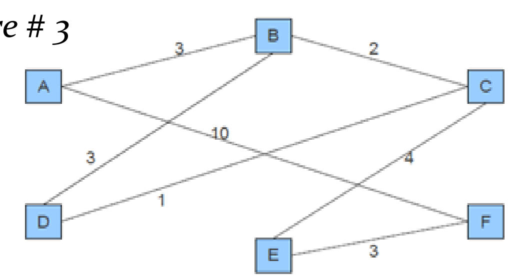


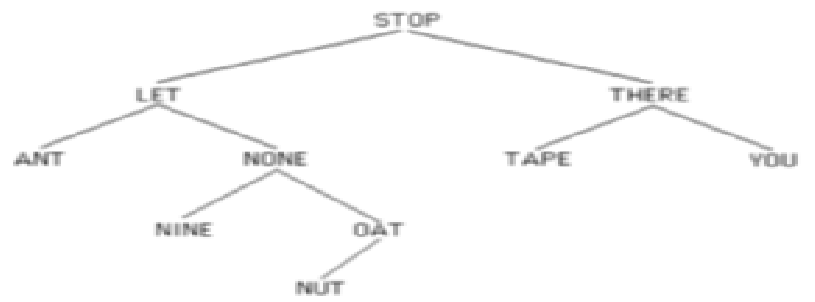
Figure # 3



(v) Set up a binary tree for the following list, in the given order, using alphabetical ordering:

STOP, LET, THERE, TAPE, NONE, YOU, ANT, NINE, OAT, NUT.

Solution:



Question # 5: Combinatorics and Pigeonhole Principle **[2x5=10 points]**

(i) There are 5 shirts all of different colors, 4 pairs of pants all of different colors, and 2 pairs of shoes with different colors. In how many ways can Ali and Bilal be dressed up with a shirt, a pair of pants, and a pair of shoes each?
Solution:

We choose 2 shirts out of 5 for both Ali and Bilal to wear, so $\binom{5}{2}2! = 20$.

We choose 2 pairs of pants out of 4 for them to wear, so $\binom{4}{2}2! = 12$.

We choose 2 pairs of shoes out of 2 for them to wear, so $\binom{2}{2}2! = 2$.

Therefore, by the rule of product, the answer is $20 \times 12 \times 2 = 480$ ways. □

(ii)
(a) Nine chairs are numbered 1 to 9. Three men and four women wish to occupy one chair each. First the men chose the chairs from amongst the chair marked 1 to 5; and then the women select the chairs from amongst the remaining. The number of possible arrangements is?
Solution:
Men can select 3 chairs from chairs numbered 1 to 5 in ${}^5C_3$ ways and remaining 6 chairs can be selected by 4 women in ${}^6C_4$ ways. Hence the required number of ways = ${}^5C_3 \times {}^6C_4$.

(b) How many different three-letter strings are there that begin with a letter A?
Solution:
While this question is asking about 3 letter initials, the first letter is already chosen for us, which is A. Therefore we only need to worry about the other two letters. There are 26 letters to choose from, and two sequential choices to make. So, there are 26^2 possible initials.

(iii) How many permutations {a, b, c, d, e, f, g} end with a?
Solution:

This is a permutation with repeats not allowed. Additionally, the last position must be an 'a', so we have only 6 items to place. Therefore, there are $P(6,6) = \frac{6!}{0!} = 720$ permutations.

A bowl contains 7 red balls and 7 blue balls. You select balls at random without looking at them. Answer the following questions (iv & v):
(iv) How many balls must you select to be sure of having at least 3 balls of the same color?
Solution: 5 balls to be sure that at least 3 balls of the same color.

(v) How many balls must you select to be sure of having at least 2 blue balls?
Solution: 9 balls to be sure that at least 2 blue balls.

Question # 6: Number Theory, Binomial theorem & Cryptography **[2x5=10 points]**

A box contains gold coins:

If the coins are equally divided among 11 friends, six coins are left over.
If the coins are equally divided among 16 friends, thirteen coins are left over.
If the coins are equally divided among 21 friends, nine coins are left over.
If the coins are equally divided among 25 friends, nineteen coins are left over.
If the box holds the smallest number of coins that meets these four conditions, how many coins are left?
In this problem, you are supposed to state and use of the following theorems:

(i)
(a) Linear congruences
(b) The Euclidean Algorithm Lemma

(ii)
(a) Bézout's Theorem
(b) Chinese Remainder Theorem

Solution:

$x \equiv 6 \pmod{11}$ $x \equiv 13 \pmod{16}$ $x \equiv 9 \pmod{21}$ $x \equiv 19 \pmod{25}$

We will follow the notation used in the proof of the Chinese remainder theorem.
We have $m = m_1 * m_2 * m_3 * m_4 = 11*16*21*25 = 92400$.
Also, by simple inspection we see that:
$y_1 = 8$ is an inverse for $M_1 = 8400$ modulo 11,
$y_2 = 15$ is an inverse for $M_2 = 5775$ modulo 16,
$y_3 = 2$ is an inverse for $M_3 = 4400$ modulo 21 and
$Y_4 = 6$ is an inverse for $M_3 = 3696$ modulo 25.
The solutions to the system are then all numbers x such that
$x = (a_1M_1y_1 + a_2M_2y_2 + a_3M_3y_3 + a_4M_4y_4) \bmod m$
$= ((6 * 8400 * 8) + (13 * 5775 * 15) + (9 * 4400 * 2) + (19*3696*6)) \bmod 92400 = 2029869 (\bmod 92400) = 89469$.
Hence, 89469 coins are left.

(iii) Use Fermat's little theorem to calculate the remainder of $2^{1,000,000}$ mod 127.

Solution:

Since $2^{126} = 1 \pmod{127}$
$= 2^{7936*126+64} \pmod{127} = (2^{126})^{7936} . 2^{64} \bmod (127) = (1)^{7936} . 2^{64} \bmod (127)$
$= 2^{64} \bmod (127) = 2^{7*9+1} \bmod 127 = (1)^{9} . 2^{1} \bmod (127) = 2$.

(iv) What is the co-efficient of x^7y^2 in the expansion of $(x + 3y)^9$.

Solution:

$$(x+3y)^9$$
$$\binom{9}{3-1} x^{9-(3-1)} (3y)^{3-1}$$
$$= \binom{9}{2} x^7 (3y)^2$$
$$= 36 \cdot x^7 \cdot 9y^2$$
$$= 324x^7y^2$$

(v) Encrypt the message "*Solution*" using the RSA system with $n = 5 \cdot 7$ and $e = 11$. Translate each letter into integers and write in the form of Cipher text equation.

Solution:

Encryption: S: $C = 18^{11} \bmod 35$. O: $C = 14^{11} \bmod 35$. L: $C = 11^{11} \bmod 35$. U: $C = 20^{11} \bmod 35$.

T: C= 19^{11} mod 35.   I: C = 08^{11} mod 35.   N: C = 13^{11} mod 35

Question # 7: Proofs, Disproof and Mathematical Induction **[2x5=10 points]**

(i) Using Direct proof method, prove that If a is an integer such that a – 2 is divisible by 3, then a^2 - 1 is divisible by 3.
Solution:
Let a – 2 is divisible by 3 for integer a. then suppose a -2 =3k,for some integer k.
Adding 3 in both side,

$a - 2 + 3 = 3k + 3$

or $a + 1 = 3(k + 1)$

or $(a+1)(a-1) = 3(k+1)(a-1)$

or $a^2 - 1 = 3m$ [for m = 3(k+1) (a -1)]

hence $a^2 - 1$ is also divisible by 3.
Therefore, by direct proof " If *a* is an integer such that a – 2 is divisible by 3, then $a^2 - 1$ is divisible by 3" *is proved.*

(ii) Using Contradiction method, prove that for integer a; if a^2 is even, then a is even.

Proposition Suppose $a \in \mathbb{Z}$. If a^2 is even, then a is even.

Proof. For the sake of contradiction, suppose a^2 is even and a is not even.
Then a^2 is even, and a is odd.
Since a is odd, there is an integer c for which $a = 2c+1$.
Then $a^2 = (2c+1)^2 = 4c^2+4c+1 = 2(2c^2+2c)+1$, so a^2 is odd.
Thus a^2 is even and a^2 is not even, a contradiction. ■

(iii) Prove by Contraposition that for integer x; if 7x + 9 is even, then x is odd.

Proposition Suppose $x \in \mathbb{Z}$. If $7x+9$ is even, then x is odd.

Proof. (Contrapositive) Suppose x is not odd.
Thus x is even, so $x = 2a$ for some integer a.
Then $7x+9 = 7(2a)+9 = 14a+8+1 = 2(7a+4)+1$.
Therefore $7x+9 = 2b+1$, where b is the integer $7a+4$.
Consequently $7x+9$ is odd.
Therefore $7x+9$ is not even. ■

(iv) Prove or disprove by counterexample: For every positive integer n, n! ≤ n^2.

n =1, n! = 1, n^2 = 1   yes
n =2, n! = 2, n^2 = 4   yes
n =3, n! = 6, n^2 = 9   yes
n =4, n! = 24, n^2 = 16   no (a counterexample)

(v) Prove using mathematical induction that $1^2 + 3^2 + 5^2 + \ldots + (2a-1)^2 = \frac{a(2a-1)(2a+1)}{3}$, whenever "a" is a nonnegative integer.
Solution:

Basis Step: Check n=1

$(2a-1)^2 = \frac{a(2a-1)(2a+1)}{3}$; $(2(1)-1)^2 = \frac{1(2(1)-1)(2(1)+1)}{3}$; 1=1

Hence P (a) is true for a =1.

<u>Inductive Step:</u> Check a = k

$1^2 + 3^2 + 5^2 + ... + (2k-1)^2 = \frac{k(2k-1)(2k+1)}{3}$

Check a =k +1

$$\boxed{\begin{aligned}(2(k+1)-1)^2 &= \frac{(k+1)(2(k+1)-1)(2(k+1)+1)}{3}\\ (2k+1)^2 &= \frac{(k+1)(2k+1)(2k+3)}{3}\end{aligned}}$$

Add $(2k+1)^2$ both side

$1^2 + 3^2 + 5^2 + ... + (2k-1)^2 + (2k+1)^2 = \frac{k(2k-1)(2k+1)}{3} + (2k+1)^2$

$= (2k+1)\{\frac{k(2k-1)+3(2k+1)}{3}\}$

$= (2k+1)\{\frac{2k^2+5k+3}{3}\}$

$= \frac{(k+1)(2k+1)(2k+3)}{3}$

Hence P (a) is true for a = k+1.

BEST OF LUCK ☺