National University of Computer & Emerging Sciences, Karachi

Fall-2020 - Department of Computer Science

Bachelor of Science (Computer Science)

Final Examination - - Solution

January 05, 2021, 03:00 pm – 06:00 pm

Course Code: CS211	Course Name: Discrete Structures
Instructor Names: Dr. Fahad Samad, Mr. Shoaib Raza and Ms. Bakhtawar Abbasi	
Student Roll No:	Section No:

Instructions:

- Return the question paper together with the answer script. Read each question completely before answering it. There are **6 questions and 4 pages.** Each question consists of **6 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 to get bonus point.

Total Time: 3 Hours **Maximum Points**: 72 Points

Question # 1: Propositional Logic, Rules of Inference, Predicate Logic and Quantifiers [2x6 =12 points]

(i) Consider the following system specifications and translate each of them into notations of propositional logic. Propositions are given as follows:

M = in Multiuser state, N = Operating normally, K = Kernel is functioning, I = in Interrupt mode

(a) The system to be in multiuser state is necessary and sufficient for system to operate normally. $M \leftrightarrow N$

(b) The kernel is functioning if the system is operating normally. $N \rightarrow K$

(c) The kernel is not functioning or the system is in interrupt mode. $\neg K \vee I$

(d) If the system is not in multiuser state, then it is in interrupt mode. $\neg M \rightarrow I$

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

$$\big((p \vee q) \wedge (p \rightarrow r)\big) \rightarrow (q \vee r)$$

Solution:

$\equiv \big((p \vee q) \wedge (p \rightarrow r)\big) \rightarrow (q \vee r)$

$\equiv \neg\big((p \vee q) \wedge (\neg p \vee r)\big) \vee (q \vee r)$ Implication Law

$\equiv \big(\neg(p \vee q) \vee \neg(\neg p \vee r)\big) \vee (q \vee r)$ De-Morgan Law

$\equiv \big((\neg p \wedge \neg q) \vee (\neg\neg p \wedge \neg r)\big) \vee (q \vee r)$ De-Morgan Law

$\equiv \big((\neg p \wedge \neg q) \vee (p \wedge \neg r)\big) \vee (q \vee r)$ Double Negation

$\equiv (\neg p \wedge \neg q) \vee q \vee (p \wedge \neg r) \vee r$ Associative and commutative law

$\equiv ((\neg p \vee q) \wedge (\neg q \vee q)) \vee ((p \vee r) \wedge (\neg r \vee r))$ Distributive Law

$\equiv ((\neg p \vee q) \wedge T) \vee ((p \vee r) \wedge T)$ Negation Law

$\equiv (\neg p \vee q) \vee ((p \vee r)$ Identity Law

$\equiv (\neg p \vee p) \vee ((q \vee r)$ Associative and commutative law

$\equiv T \vee (q \vee r)$ Negation Law

$\equiv T$ Domination Law

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

((¬r → (s → ¬t)) ∧ (¬r ∨ w) ∧ (¬p → s) ∧ (¬w)) → (t → p)

Solution:

Assertion	Reasons
1. ¬w 2. ¬r ∨ w 3. ¬r 4. ¬r→(s → ¬t) 5. s → ¬t 6. ¬p → s 7.¬p → ¬t 8. t → p	1. Hypothesis 2. Hypothesis 3. Disjunctive syllogism 4. Hypothesis 5. Modus ponens of (3) and (4) 6.Hypothesis 7. Hypothetical syllogism of (6) and (5) 8. contrapositive of (7)

Suppose F (p, q) is the predicate "**p understands q**", the universe of discourse for p is "the set of students in your class", and the universe of discourse for q is "the set of examples in the lecture notes."(For parts (iv) & (v) only)

(iv) Write the following predicate expressions in good English without using variables in your answers:
(a) $\exists p \, \forall q \, F(p, q)$
Solution: There exists a student in this class who understands every example in the lecture notes.
(b) $\forall q \, \exists p \, F(p, q)$
Solution: For every example in the lecture notes there is a student in the class who understands that example.

(v) Write the predicate expressions of the following statements using variables and any needed quantifiers:
(a) Every student in this class understands at least one example in the notes." Solution: $\forall p \, \exists q \, F(p, q)$
(b) There is an example in the notes that every student in this class understands." Solution: $\exists q \, \forall p \, F(p, q)$

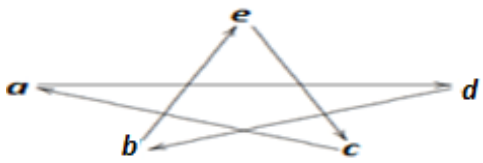
(vi) Determine the truth value of each of these statements if the domain for all variables consists of all real numbers.
(a) $\forall x \, \exists y \, (x^2 = y)$ Solution: True
(b) $\forall x \, \exists y \, (x = y^2)$ Solution: False

QUESTION # 2: Set Theory, Relations and Functions [2x6 =12 points]

(i) Let ***X*** and ***Y*** be two sets. Prove or disprove using the set builder notation that $\boldsymbol{X - (X \cap Y) = (X - Y).}$
Solution:

$\equiv \{x| \, (x \in X) \cap x \notin (X \cap Y)\}$ $A - B = A \cap B^c$
$\equiv \{x| \, (x \in X) \wedge x \notin (X \wedge Y)\}$
$\equiv \{x| \, (x \in X) \wedge \neg x \in (X \wedge Y)\}$
$\equiv \{x| \, (x \in X) \wedge (x \notin X) \vee (x \notin Y)\}$ Distributive law
$\equiv \{x|((x \in X) \wedge (x \notin X)) \vee ((x \in X) \wedge (x \notin Y))\}$
$\equiv \{x|(\emptyset) \vee ((x \in X) \wedge (x \notin Y))\}$ Complement Law
$\equiv \{x| \, (x \in X) \wedge (x \notin Y)\}$ $A - B = A \cap B^c$
$\equiv \{x| \, (x \in (X - Y)\}$

(ii) Let R be the relation on {a, b, c, d, e} represented by the digraph shown in figure 1. What is $R \circ R$? (draw digraph).
Solution:
R= {(e,c), (c,a), (a,d), (d,b), (b,e)}



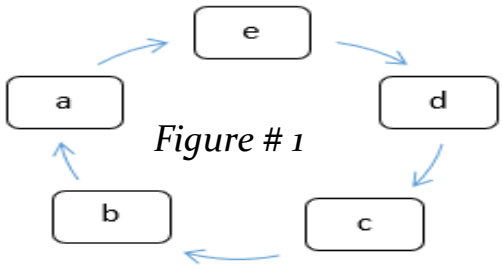


Figure # 1

(iii) A tournament graph G = (V, E) is a directed graph such that there is either an edge from u to v or an edge from v to u for every distinct pair of nodes u and v. (The nodes represent players and an edge u → v indicates that player u beats player v.) 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:

1. **transitive**

   Solution. 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. ■

2. **symmetric**

   Solution. The "beats" relation is not symmetric by the definition of a tournament: if x beats y then y does not beat x. ■

3. **antisymmetric**

   Solution. The "beats" relation is antisymmetric since for any distinct players x and y, if x beats y then y does not beat x. ■

4. **reflexive**

   Solution. The "beats" relation is not reflexive since a tournament graph has no self-loops. ■

(iv) Consider the function g: Z⟶Z defined by $g(n)=n^2+1$. Find g (1) and g ({1}). Is g (1) = g ({1}) are equal if not why?
Solution:

Note that $g(1) \neq g(\{1\})$. The first is an element: $g(1) = 2$. The second is a set: $g(\{1\}) = \{2\}$.

(v) 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?

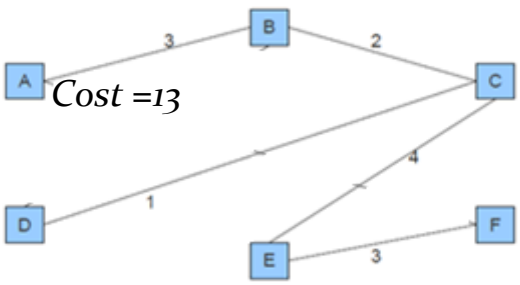
Yes! In fact, this process will always end because we have $\mathbb{N}$ as our domain, so there is a least element. And we gave the value of $f(0)$ explicitly, so we are good. In fact, we might decide to work up to $f(6)$ instead of working down from $f(6)$:

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

(vi) How many functions are there from a set with four elements to a set with three elements?
Solution:
Hence 3 * 3 * 3* 3 = 81 different functions from a set with three elements to a set with four elements.

<u>Question # 3: Graph Theory and Trees</u> **[2x6=12 points]**

(i) Construct the Minimum spanning tree (MST) for the given graph in figure # 2 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.



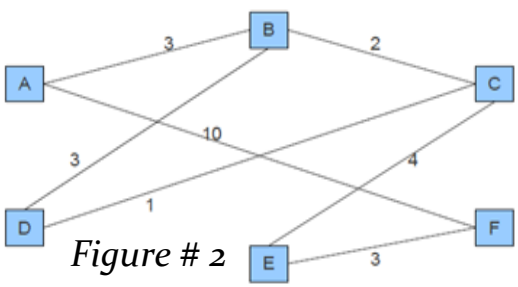
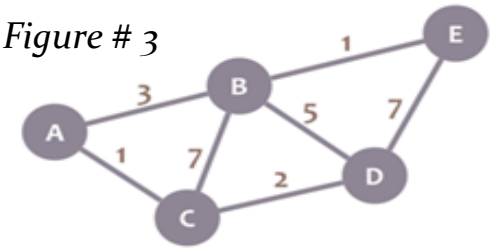


Figure # 2

(ii) Find the Shortest path from Node C to all other nodes in graph as shown in figure # 3 using Dijkstra's algorithm.

Node	D(A)	D(B)	D(D)	D(E)
C	1, C	7, C	2, C	∞
CA	-	4, A	2, C	∞
CAD	-	4, A	-	9, D
CADB	-	-	-	5, B
CADBE				

Figure # 3



(iii) Below is a graph as shown in figure # 4 representing friendships between a group of students (each vertex is a student and each edge is a friendship). Is it possible for the students to sit around a round table in such a way that every student sits between two friends? What does this question have to do with paths?

Solution:

We are looking for a Hamiltonian cycle, and this graph does have one.

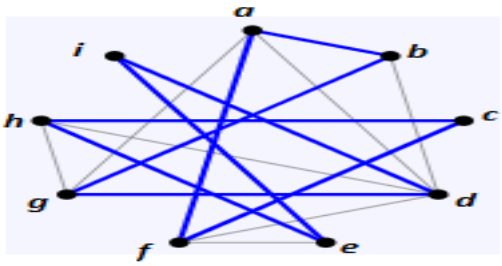
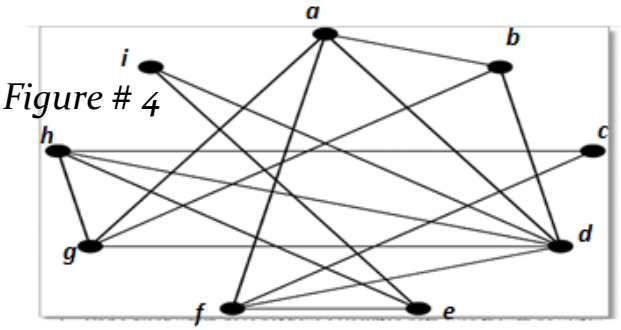
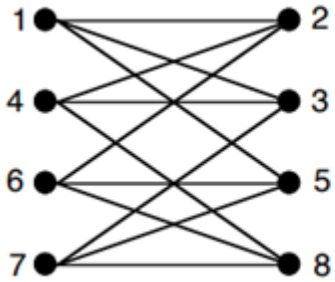


Figure # 4

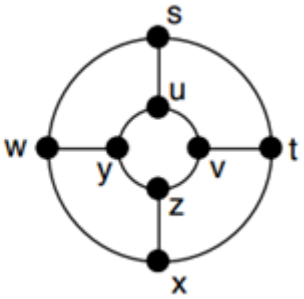


(iv) Determine if the following two graphs G and H are isomorphic as shown in figure # 5. If they are, give function F: V (G) ⟶ V (H) that define the isomorphism. If they are not, give the reason why?



G

Figure # 5



H

Solution:

F(1)= s, F(2)= t, F(3)= u, F(4)= v, F(5)= w, F(6)= x, F(7)= y, F(8)= z.

(v) Construct Pre-order, Post-order and In-order traversals of the given tree as shown in figure # 6.

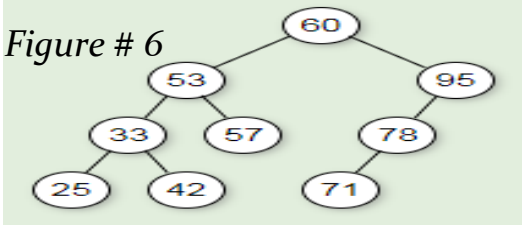
Solution:

Pre-order: 60 53 33 25 42 57 95 78 71

Post-order: 25 42 33 57 53 71 78 95 60

In-order: 25 33 42 53 57 60 71 78 95

Figure # 6



(vi) Convert the given expression into postfix and prefix notations. (A + B) * C - (D - E) * (F + G).

Solution:

Prefix notation: – * + A B C * – D E + F G

Postfix notation: A B + C * D E – F G + * –

Question # 4: Combinatorics and Discrete Probability **[2x6=12 points]**

Suppose that you roll five 6-sided dice that are fair and mutually independent. (For parts (i) & (ii) only)

(i) What is the probability that all five dice show different values?
Example: (1, 2, 3, 4, 5) is a roll of this type, but (1, 1, 2, 3, 4) is not.

Solution. The probability space is the uniform distribution on the 6^5 possible numbers rolled on the five (distinguishable) dice. So the probability that all dice are different is the number of outcomes in which the dice have distinct values divided by 6^5. There are $(6)_5 = 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2$ such outcomes so

$$\Pr(\text{all rolls distinct}) = \frac{6 \cdot 5 \cdot 4 \cdot 3 \cdot 2}{6^5} = \frac{5!}{6^4}$$

An alternative approach uses the observation that the conditional probability that the $i+1$st die value differs from the preceding rolls, given that the first i values differ, is $(6-i)/6$ for $1 \leq i \leq 4$, and the probability that all five values are different is the product of these conditional probabilities, namely

$$\Pr(\text{all rolls distinct}) = \frac{5}{6} \cdot \frac{4}{6} \cdot \frac{3}{6} \cdot \frac{2}{6} = \frac{5!}{6^4}$$

(ii) What is the probability that two dice show the same value and the remaining three dice all show different values?
Example: (6, 1, 6, 2, 3) is a roll of this type, but (1, 1, 2, 2, 3) and (4, 4, 4, 5, 6) are not.

Solution. There are $\binom{5}{2}$ possible pairs of rolls that might have the same value and 6 possibilities for what this value is. There $5 \cdot 4 \cdot 3$ possible distinct values for the remaining three rolls. So

$$\Pr(\text{exactly two values the same}) = \frac{\binom{5}{2} \cdot 6 \cdot 5 \cdot 4 \cdot 3}{6^5} = \frac{100}{6^3}$$

An alternative way to count is: there are $\binom{6}{4}$ sets of four values among the five dice, 4 choices for which of these values is repeated, and by the Bookkeeper rule, $\binom{5}{2,1,1,1} = 5!/2$ permutations of a sequence consisting of five values, one of which appears twice. So,

$$\Pr(\text{exactly two values the same}) = \frac{\binom{6}{4} \cdot 4 \cdot 5!/2}{6^5} = \frac{100}{6^3}$$

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

(iv) How many ways are there of choosing k things from {1 . . . n} if 1 and 2 can't both be chosen? (Suppose n, k ≥ 2.)
Solution:

First find all the ways of choosing k things from n—$C(n,k)$. Then subtract the number of those ways in which both 1 and 2 are chosen:

- This amounts to choosing $k-2$ things from $\{3, \ldots, n\}$: $C(n-2, k-2)$.

Thus, the answer is

$$C(n,k) - C(n-2, k-2)$$

(v) How many ways are there to distribute four distinct balls evenly between two distinct boxes (two balls go in each box)?
Solution:
All you need to decide is which balls go in the first box. C(4, 2) = 6

(vi) Suppose that all license plates have three uppercase letters followed by three digits.
(a) How many license plates begin with B and end in 1?
Solution:
Solution:
Begins with B & end with 1: 1*26*26*10*10*1=67600

(b) How many license plates are possible in which all the letters and digits are distinct?
Solution:
Distinct License plates= 26*25*24*10*9*8 = 11,232,000.

Question # 5: Number theory, Binomial theorem and Pigeon hole Principle [2x6=12 points]

(i) A shipwrecked sailor passes the time of day by counting the coconuts he has gathered. When he counts by threes, there are 2 coconuts left over. When he counts by fives, there are 4 left over, and when he counts by sevens, there are 5 left over, and when he counts by eleven, there is only one coconut left. How many coconuts has the sailor gathered if he is positive that he had fewer than 150 coconuts.
In this problem, you are supposed to state and use of the following Theorems:
a. Chinese Remainder Theorem
b. The Euclidean Algorithm Lemma
c. Bézout's Theorem
d. Linear congruences
Solution:
$x \equiv 2 \pmod 3$ $x \equiv 4 \pmod 5$ $x \equiv 5 \pmod 7$ $x \equiv 1 \pmod{11}$
We will follow the notation used in the proof of the Chinese remainder theorem.
We have $m=m_1 * m_2 * m_3 * m_4 = 3*5*7*11=1155$.
Also, by simple inspection we see that:
$y_1 = 1$ is an inverse for $M_1 = 385$ modulo 3,
$y_2 = 1$ is an inverse for $M_2 = 231$ modulo 5,
$y_3 = 2$ is an inverse for $M_3 = 165$ modulo 7 and
$Y_4 = 2$ is an inverse for $M_3 = 105$ modulo 11.
The solutions to the system are then all numbers x such that
$x = (a_1M_1y_1 + a_2M_2y_2 + a_3M_3y_3 + a_4M_4y_4) \bmod m$
$= ((2 * 385 * 1) + (4* 231* 1) + (5* 165* 2) + (1*105*2)) \bmod 2310 = 3554 \pmod{1155} = 89.$
Hence, he has 89 coconuts.

(ii) Use Fermat's little theorem to calculate the remainder of $9^{2579} \bmod 79$.
Solution:
Solution:
Since $9^{78} = 1 \pmod{79}$
$= 9^{78*33+5} \pmod{79} = (9^{78})^{33} .9^5 \bmod (79) = (1)^{33} .9^5 \bmod (79)$
$= 9^5 \bmod 79 = 59049 \bmod 79 = 36.$

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

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

Suppose that every student in a discrete mathematics class of 25 students is a freshman, a sophomore, or a junior.

(iv) Show that there are at least nine freshmen, at least nine sophomores or at least nine juniors in the class.
Solution:
If there are less than or equal 8 freshmen, less than or equal 8 sophomores, and less than or equal 8 juniors in the class, then altogether there are no more than 24 students in the class, which is not the case. Therefore, our assumption is wrong, and there are at least 9 freshmen, at least 9 sophomores, or at least 9 juniors in the class.

(v) Show that there are either at least three freshmen, at least 19 sophomores, or at least five juniors in the class.
Solution:
If there are less than or equal 2 freshmen, less than or equal 18 sophomores, and less than or equal 4 juniors in the class, then altogether there are no more than 24 students in the class, which is not the case. Therefore, our assumption is wrong, and there are either at least 3 freshmen, at least 19 sophomores, or at least 5 juniors in the class.

(vi) Find the check digit of the following Universal Product Code (UPC): 69277198116.
Solution:
$3x_1 + x_2 + 3x_3 + x_4 + 3x_5 + x_6 + 3x_7 + x_8 + 3x_9 + x_{10} + 3x_{11} + x_{12} \equiv 0 \pmod{10}$.
$3*6+ 9 + 3*2 + 7 + 3*7 + 1 + 3*9 + 8 + 3*1 + 1 + 3*6 + x_{12} \equiv 0 \pmod{10}$.
$119 + x_{12} \equiv 0 \pmod{10}$.
$x_{12} \equiv 0 \pmod{10}$ So, the check digit is 1.

Question # 6: Proofs, Mathematical Induction and Cryptography **[2x6=12 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 there are no integer x and y such that $x^2 = 4y + 2$.

Solution:

Proof. We proceed by contradiction. So suppose there *are* integers x and y such that $x^2 = 4y + 2 = 2(2y + 1)$. So x^2 is even. We have seen that this implies that x is even. So $x = 2k$ for some integer k. Then $x^2 = 4k^2$. This in turn gives $2k^2 = (2y + 1)$. But $2k^2$ is even, and $2y + 1$ is odd, so these cannot be equal. Thus we have a contradiction, so there must not be any integers x and y such that $x^2 = 4y + 2$. QED

(iii) Prove by Contraposition that for all integers a and b, if a + b is odd then a is odd or b is odd.

Solution:

The problem with trying a direct proof is that it will be hard to separate a and b from knowing something about $a + b$. On the other hand, if we know something about a and b separately, then combining them might give us information about $a + b$. The contrapositive of the statement we are trying to prove is: for all integers a and b, if a and b are even, then $a + b$ is even. Thus our proof will have the following format:

Let a and b be integers. Assume that a and b are both even. la la la. Therefore $a + b$ is even.

Here is a complete proof:

Proof. Let a and b be integers. Assume that a and b are even. Then $a = 2k$ and $b = 2l$ for some integers k and l. Now $a + b = 2k + 2l = 2(k + 1)$. Since $k + l$ is an integer, we see that $a + b$ is even, completing the proof. QED

(iv) Prove using mathematical induction that $1^3 + 2^3 + 3^3 + \ldots + n^3 = \left(\frac{n(n+1)}{2}\right)^2$ whenever n is a nonnegative integer.

Solution:

$1^3 + 2^3 + 3^3 + \ldots + n^3 = (n (n + 1) / 2)^2$

STEP 1: We first show that p (1) is true.

Left Side = $1^3 = 1$

Right Side = $1^2 (1 + 1)^2 / 4 = 1$

hence p (1) is true.

STEP 2: We now assume that p (k) is true

$1^3 + 2^3 + 3^3 + \ldots + k^3 = (k (k + 1) / 2)^2$ (1)

add $(k + 1)^3$ to both sides

$1^3 + 2^3 + 3^3 + \ldots + k^3 + (k + 1)^3 = [(k+1) (k+1+ 1) / 2)]^2$

$1^3 + 2^3 + 3^3 + \ldots + k^3 + (k + 1)^3 = [(k+1) (k+2) / 2)]^2$ (2)

put eq(1) in eq(2)

$\Rightarrow (k (k + 1) / 2)^2 + (k + 1)^3 = [(k+1) (k+2) / 2)]^2$

$\Rightarrow k^2 (k + 1)^2 /4 + (k + 1)^3$

$\Rightarrow (k + 1)^2 [k^2 + 4 k + 4] / 4$

$\Rightarrow (k + 1)^2 [(k + 2)^2] / 4$

$\Rightarrow [(k+1) (k+2) / 2)]^2 = [(k+1) (k+2) / 2)]^2$

LHS = RHS, Hence proved!

(v) Prove or disprove by counterexample: The sum of squares of two numbers is an odd number.
Solution:

$1^2 + 2^2 = 1 + 4 = 5$	True
$3^2 + 4^2 = 9 + 16 = 25$	True
$1^2 + 3^2 = 1 + 9 = 10$	False

Hence, it's a disproof.

(vi) Jack is sending Tommy a message with RSA. The public key is 3, while n = p*q is 55. What is the value of d that Tommy must use to decrypt the message?
Hint: Public key <e, n> and Private Key <d, n>
Solution:
If N = 55, then p = 5 and q = 11, as these are the only two primes whose product is equal to 55.
Next, we want $d = e^{-1} \bmod (p-1)(q-1)$. To do this, we must run the extended-gcd algorithm.
1 = 40 - 3(13)
1 = 40(1) + 3(-13)
So, d = -13, which, mod 40, is 27.

BEST OF LUCK ☺