

FAST- National University of Computer and Emerging Sciences, Karachi.

FAST School of Computing

Fall 2021, Assignment # 2 -- Solution

CS1005-Discrete Structures

Instructions:

Max. Points: 100

- 1- This is hand written assignment.
- 2- Just write the question number instead of writing the whole question.
- 3- You can only use A4 size paper for solving the assignment.

1. Let R be the following relation defined on the set $\{a, b, c, d\}$:

$$R = \{(a, a), (a, c), (a, d), (b, a), (b, b), (b, c), (b, d), (c, b), (c, c), (d, b), (d, d)\}$$

Determine whether R is:

- | | | |
|----------------|-----------------|-------------------|
| (a) Reflexive: | (b) Symmetric | (c) Antisymmetric |
| (d) Transitive | (e) Irreflexive | (f) Asymmetric |

Solution:

- (a) R is reflexive because R contains (a, a) , (b, b) , (c, c) , and (d, d) .
- (b) R is not symmetric because R contains (a, c) but not $(c, a) \in R$.
- (c) R is not antisymmetric because both $(b, c) \in R$ and $(c, b) \in R$, but $b \neq c$.
- (d) R is not Transitive because both $(a, c) \in R$ and $(c, b) \in R$, but not $(a, b) \in R$.
- (e) R is not irreflexive because R contains (a, a) , (b, b) , (c, c) , and (d, d) .
- (f) R is not Asymmetric because R is not Antisymmetric.

2. Let R be the following relation on the set of real numbers:

$$aRb \leftrightarrow \lfloor a \rfloor = \lfloor b \rfloor, \text{ where } \lfloor x \rfloor \text{ is the floor of } x.$$

Determine whether R is:

- | | | |
|----------------|-----------------|-------------------|
| (a) Reflexive | (b) Symmetric | (c) Antisymmetric |
| (d) Transitive | (e) Irreflexive | (f) Asymmetric |

Solution:

- (a) R is reflexive: $a = a$ is true for all real numbers.
- (b) R is symmetric: suppose $a = b$; then $b = a$.
- (c) R is not antisymmetric: we can have aRb and bRa for distinct a and b . For example, $1.1 = 1.2$
- (d) R is Transitive because for any real numbers, a , b , and c , if $(a, b), (b, c) \in R$ then $a = b$ and $b = c$. This implies $a = c$ by substitution, so $(a, c) \in R$.
- (e) R is not irreflexive because $a = a$ is true for all real numbers.
- (f) R is not Asymmetric because R is not Antisymmetric.

3. List the ordered pairs in the relation R from $A = \{0, 1, 2, 3, 4\}$ to $B = \{0, 1, 2, 3\}$, where $(a, b) \in R$ if and only if

- | | | |
|-----------------|-----------------------|-----------------------------|
| a) $a = b$. | b) $a + b = 4$. | c) $a > b$. |
| d) $a \mid b$. | e) $\gcd(a, b) = 1$. | f) $\text{lcm}(a, b) = 2$. |

Solution:

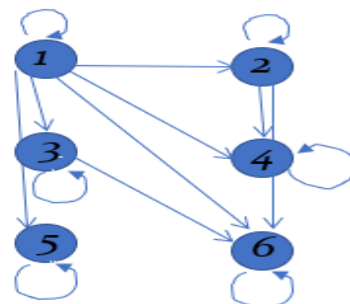
- a) $\{(0, 0), (1, 1), (2, 2), (3, 3)\}$
- b) $\{(1, 3), (2, 2), (3, 1), (4, 0)\}$
- c) $\{(1, 0), (2, 0), (3, 0), (4, 0), (2, 1), (3, 1), (3, 2), (4, 1), (4, 2), (4, 3)\}$
- d) $\{(1, 0), (2, 0), (3, 0), (4, 0), (1, 1), (1, 2), (2, 2), (1, 3), (3, 3)\}$
- e) $\{(1, 0), (0, 1), (1, 1), (1, 2), (1, 3), (2, 1), (3, 1), (4, 1), (2, 3), (3, 2), (4, 3)\}$
- f) $\{(1, 2), (2, 1), (2, 2)\}$

4. List all the ordered pairs in the relation $R = \{(a, b) \mid a \text{ divides } b\}$ on the set $\{1, 2, 3, 4, 5, 6\}$. Display this relation as Directed Graph(digraph), as well in matrix form.

mSolution:

$R = \{(1, 1), (1, 2), (1, 3), (1, 4), (1, 5), (1, 6), (2, 2), (2, 4), (2, 6), (3, 3), (3, 6), (4, 4), (5, 5), (6, 6)\}$

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{bmatrix}$$



5. For each of these relations on the set $\{1, 2, 3, 4\}$, decide whether it is reflexive, whether it is symmetric, whether it is antisymmetric, and whether it is transitive.

a) $\{(2, 2), (2, 3), (2, 4), (3, 2), (3, 3), (3, 4)\}$

Solution:

- (a) R is not reflexive: It doesn't contain $(1,1)$ and $(4,4)$.
- (b) R is not symmetric because R contains $(2, 4)$ but not $(4, 2) \in R$.
- (c) R is not antisymmetric: we have $(2,3)$ and $(3,2)$ but $2 \neq 3$.
- (d) R is Transitive because for any numbers a, b, and c, if $(a, b), (b, c) \in R$ then $(a, c) \in R$.

b) $\{(1, 1), (1, 2), (2, 1), (2, 2), (3, 3), (4, 4)\}$

Solution:

- (a) R is reflexive: It contains $(1,1), (2,2), (3,3)$ and $(4,4)$.
- (b) R is symmetric because (a,b) and $(b,a) \in R$.
- (c) R is not antisymmetric: we have $(1,2)$ and $(2,1)$ but $1 \neq 2$.
- (d) R is Transitive because for any numbers a, b, and c, if $(a, b), (b, c) \in R$ then $(a, c) \in R$.

c) $\{(2, 4), (4, 2)\}$

Solution:

- (a) R is not reflexive: It doesn't contain $(1,1), (2,2), (3,3)$ and $(4,4)$.
- (b) R is symmetric because R contains $(2, 4)$ and $(4, 2) \in R$.
- (c) R is not antisymmetric: we have $(2,4)$ and $(4,2)$ but $2 \neq 4$.
- (d) R is not Transitive because $(2,4), (4, 2) \in R$ but not $(2,2) \in R$.

d) $\{(1, 2), (2, 3), (3, 4)\}$

Solution:

- (a) R is not reflexive: It doesn't contain $(1,1), (2,2), (3,3)$ and $(4,4)$.
- (b) R is not symmetric because $(1,2) \in R$ but not $(2,1) \in R$.
- (c) R is antisymmetric: we have (a,b) but not $(b,a) \in R$.
- (d) R is not Transitive because $(1,2), (2, 3) \in R$ but not $(1,3) \in R$.

e) $\{(1, 1), (2, 2), (3, 3), (4, 4)\}$

Solution:

- (a) R is reflexive: It contains $(1,1), (2,2), (3,3)$ and $(4,4)$.
- (b) R is symmetric because R contains (a,b) and $(b,a) \in R$.
- (c) R is antisymmetric: we have (a,b) and $(b,a) \in R$ then $a = b$.
- (d) R is Transitive because for any numbers a, b, and c, if $(a, b), (b, c) \in R$ then $(a, c) \in R$.

f) $\{(1, 3), (1, 4), (2, 3), (2, 4), (3, 1), (3, 4)\}$

Solution:

- (a) R is not reflexive: It doesn't contain $(1,1)$, $(2,2)$, $(3,3)$ and $(4,4)$.
- (b) R is not symmetric because $(1,4) \in R$ but not $(4,1) \in R$.
- (c) R is not antisymmetric: we have $(1,3)$ and $(3,1) \in R$ but $1 \neq 3$.
- (d) R is not Transitive because we have $(1,3)$ and $(3,1) \in R$ but not $(1,1) \in R$.

6. Determine whether the relation R on the set of all people is reflexive, symmetric, antisymmetric, Asymmetric, irreflexive and/or transitive, where $(a, b) \in R$ if and only if:
- a) a is taller than b .

Solution:

The relation R is **not reflexive**, because a person cannot be taller than himself/herself.

The relation R is **not symmetric**, because if person A is taller than person B , then person B is NOT taller than person A .

The relation R is **antisymmetric**, because $(a, b) \in R$ and $(b, a) \in R$ cannot occur at the same time (as one person is always taller than the other, but not the other way around).

The relation R is **transitive**, because if person A is taller than person B and if person B is taller than person C , then person A needs to be taller than person C as well.

- b) a and b were born on the same day.

Solution:

The relation R is **reflexive**, because a person is born on the same day as himself/herself.

The relation R is **symmetric**, because if person A and person B are born on the same day, then person B is also born on the same day as person A .

The relation R is **not antisymmetric**, because if person A and person B are born on the same day and if person B and person A are born on the same day, then these two people are not necessarily the same person.

The relation R is **transitive**, because if person A and person B are born on the same day and if person B and person C are born on the same day, then person A and person C are also born on the same day.

- c) a has the same first name as b .

Solution:

The relation R is **reflexive**, because a person has the same first name as himself/herself.

The relation R is **symmetric**, because if person A has the same first name as person B , then person B also has the same first name as person A .

The relation R is **not antisymmetric**, because if person A has the same first name as person B and if person B also has the same first name as person A , then these two people are not necessarily the same person (as there are different people with the same first name).

The relation R is **transitive**, because if person A has the same first name as person B and if person B also has the same first name as person C , then person A also has the same first name as person C .

- d) a and b have a common grandparent.

Solution:

The relation R is **reflexive**, because a person has the same grandparents as himself/herself.

The relation R is **symmetric**, because if person A and person B have a common grandparent, then person B and person A also have a common grandparent.

The relation R is **not antisymmetric**, because if person A and person B have a common grandparent and if person B and person A have a common grandparent, then these two people are not necessarily the same person (as there are different people with the same grandparents).

The relation R is **not transitive**, because if person A and person B have a common grandparent and if person B and person C have a common grandparent, then person A and person C do not necessarily have a common grandparent (for example, the common grandparent of A and B can be from person B's father's side of the family, while the common grandparent of B and C can be from person B's mother's side of the family).

- (a) Antisymmetric, Irreflexive, Asymmetric and Transitive
- (b) Reflexive, Symmetric and Transitive
- (c) Reflexive, Symmetric and Transitive
- (d) Reflexive and Symmetric

7. Give an example of a relation on a set that is
a) both symmetric and antisymmetric.

Solution:

$$\{ (1,1), (2,2), (3,3), (4,4) \}$$

- b) neither symmetric nor antisymmetric.

Solution:

$$\{ (1,2), (2,1), (3,4) \}$$

8. Consider these relations on the set of real numbers: $A = \{1,2,3\}$

$R_1 = \{(a, b) \in R \mid a > b\}$, the "greater than" relation,

$R_2 = \{(a, b) \in R \mid a \geq b\}$, the "greater than or equal to" relation,

$R_3 = \{(a, b) \in R \mid a < b\}$, the "less than" relation,

$R_4 = \{(a, b) \in R \mid a \leq b\}$, the "less than or equal to" relation,

$R_5 = \{(a, b) \in R \mid a = b\}$, the "equal to" relation,

$R_6 = \{(a, b) \in R \mid a \neq b\}$, the "unequal to" relation.

Find:

a) $R_2 \cup R_4$.

b) $R_3 \cup R_6$.

c) $R_3 \cap R_6$.

d) $R_4 \cap R_6$.

e) $R_3 - R_6$.

f) $R_6 - R_3$.

g) $R_2 \oplus R_6$.

h) $R_3 \oplus R_5$.

i) $R_2 \circ R_1$.

j) $R_6 \circ R_6$.

Solution:

$$R_1 = \{ (2,1), (3,1), (3,2) \}$$

$$R_2 = \{ (1,1), (2,2), (3,3), (2,1), (3,1), (3,2) \}$$

$$R_3 = \{ (1,2), (1,3), (2,3) \}$$

$$R_4 = \{ (1,1), (2,2), (3,3), (1,2), (1,3), (2,3) \}$$

$$R_5 = \{ (1,1), (2,2), (3,3) \}$$

$$R_6 = \{ (1,2), (1,3), (2,1), (2,3), (3,1), (3,2) \}$$

a) $R_2 \cup R_4 = \{ (1,1), (2,2), (3,3), (2,1), (3,1), (3,2), (1,2), (1,3), (2,3) \}$

b) $R_3 \cup R_6 = \{ (1,2), (1,3), (2,1), (2,3), (3,1), (3,2) \}$

c) $R_3 \cap R_6 = \{ (1,2), (1,3), (2,3) \}$

d) $R_4 \cap R_6 = \{ (1,2), (1,3), (2,3) \}$

e) $R_3 - R_6 = \{ \}$ OR Φ

- f) $R_6 - R_3 = \{ (2,1), (3,1), (3,2) \}$
g) $R_2 \oplus R_6 = \{ (1,1), (2,2), (3,3), (1,2), (1,3), (2,3) \}$
h) $R_3 \oplus R_5 = \{ (1,1), (2,2), (3,3), (1,2), (1,3), (2,3) \}$
i) $R_2 \circ R_1 = \{ (2,1), (3,1), (3,2) \}$
j) $R_6 \circ R_6 = \{ (1,1), (2,2), (3,3), (2,1), (3,1), (3,2), (1,2), (1,3), (2,3) \}$

9. (a) Represent each of these relations on $\{1, 2, 3\}$ with a matrix (with the elements of this set listed in increasing order).

i) $\{ (1, 1), (1, 2), (1, 3) \}$

Solution:
$$\begin{bmatrix} 1 & 1 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix}$$

ii) $\{ (1, 2), (2, 1), (2, 2), (3, 3) \}$

Solution:
$$\begin{bmatrix} 0 & 1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{bmatrix}$$

iii) $\{ (1, 1), (1, 2), (1, 3), (2, 2), (2, 3), (3, 3) \}$

Solution:
$$\begin{bmatrix} 1 & 1 & 1 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}$$

iv) $\{ (1, 3), (3, 1) \}$

Solution:
$$\begin{bmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{bmatrix}$$

(b) List the ordered pairs in the relations on $\{1, 2, 3\}$ corresponding to these matrices (where rows and columns correspond to the integers listed in increasing order).

(i) $\begin{bmatrix} 1 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 1 \end{bmatrix}$ Solution: $R = \{ (1,1), (1,3), (2,2), (3,1), (3,3) \}$

(ii) $\begin{bmatrix} 0 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 1 & 0 \end{bmatrix}$ Solution: $R = \{ (1,2), (2,2), (3,2) \}$

(iii) $\begin{bmatrix} 1 & 1 & 1 \\ 1 & 0 & 1 \\ 1 & 1 & 1 \end{bmatrix}$ Solution: $R = \{ (1,1), (1,2), (1,3), (2,1), (2,3), (3,1), (3,2), (3,3) \}$

10. (a) Suppose that R is the relation on the set of strings of English letters such that aRb if and only if $l(a) = l(b)$, where $l(x)$ is the length of the string x . Is R an equivalence relation?

Solution:

Show that all of the properties of an equivalence relation hold.

- Reflexivity: Because $l(a) = l(a)$, it follows that aRa for all strings a .
- Symmetry: Suppose that aRb . Since $l(a) = l(b)$, $l(b) = l(a)$ also holds and bRa .
- Transitivity: Suppose that aRb and bRc . Since $l(a) = l(b)$, and $l(b) = l(c)$, $l(a) = l(c)$ also holds and aRc .

(b) Let m be an integer with $m > 1$. Show that the relation $R = \{ (a,b) \mid a \equiv b \pmod{m} \}$ is an equivalence relation on the set of integers.

Solution:

Recall that $a \equiv b \pmod{m}$ if and only if m divides $a - b$.

- Reflexivity: $a \equiv a \pmod{m}$ since $a - a = 0$ is divisible by m since $0 = 0 \cdot m$.
- Symmetry: Suppose that $a \equiv b \pmod{m}$. Then $a - b$ is divisible by m , and so $a - b = km$, where k is an integer. It follows that $b - a = (-k)m$, so $b \equiv a \pmod{m}$.
- Transitivity: Suppose that $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$. Then m divides both $a - b$ and $b - c$. Hence, there are integers k and l with $a - b = km$ and $b - c = lm$. We obtain by adding the equations: $a - c = (a - b) + (b - c) = km + lm = (k + l)m$. Therefore, $a \equiv c \pmod{m}$.

(c) Let m be a positive integer. Show that $a \equiv b \pmod{m}$ if $a \bmod m = b \bmod m$.

Solution:

Proof:(Note: because this theorem is a biconditional, we must prove it in “both directions.”)

First, assume $a \equiv b \pmod{m}$

then $m \mid (a-b)$, so there is $k \in \mathbb{Z}$ such that $a - b = mk$.

Let $a \bmod m = r$.

Then, according to the division algorithm, there is $q \in \mathbb{Z}$ such that $a = mq + r$, $0 \leq r < m$.

Using $a = mq + r$ to replace a in $a - b = mk$, we get

$$mq + r - b = mk$$

So

$$mq - mk + r = b$$

$$m(q - k) + r = b$$

This shows that r is the remainder when b is divided by m , so $b \bmod m = r (= a \bmod m)$. We have proven that if $a \equiv b \pmod{m}$ then $a \bmod m = b \bmod m$.

Conversely, assume $a \bmod m = b \bmod m$.

Let $r = a \bmod m = b \bmod m$.

Then, according to the division algorithm, there are $q_1, q_2 \in \mathbb{Z}$ such that

$$a = mq_1 + r,$$

$$b = mq_2 + r, \quad 0 \leq r < m.$$

$$\text{Then } a - b = mq_1 + r - (mq_2 + r)$$

$$= mq_1 + r - mq_2 - r$$

$$= mq_1 - mq_2$$

$$= m(q_1 - q_2) \quad \text{This shows that } m \mid (a-b), \text{ so } a \equiv b \pmod{m}.$$

We have proven that if $a \bmod m = b \bmod m$ then $a \equiv b \pmod{m}$.

11. What are the quotient and remainder when:

- | | | | |
|---------------------------|-----------|------------|----------|
| a) 19 is divided by 7? | Solution: | $q = 2;$ | $r = 5$ |
| b) -111 is divided by 11? | Solution: | $q = -11;$ | $r = 10$ |
| c) 789 is divided by 23? | Solution: | $q = 34;$ | $r = 7$ |
| d) 1001 is divided by 13? | Solution: | $q = 77;$ | $r = 0$ |
| e) 10 is divided by 19? | Solution: | $q = 0;$ | $r = 10$ |
| f) 3 is divided by 5? | Solution: | $q = 0;$ | $r = 3$ |
| g) -1 is divided by 3? | Solution: | $q = -1;$ | $r = 2$ |
| h) 4 is divided by 1? | Solution: | $q = 4;$ | $r = 0$ |

12. (a) Find $a \div m$ and $a \bmod m$ when

$$q = a \div m$$

$$r = a \bmod m$$

i) $a = -111, m = 99.$	Solution: $-2 = -111 \div 99$; $87 = -111 \div 99$
ii) $a = -9999, m = 101.$	Solution: $-99 = -9999 \div 101$; $0 = -9999 \div 101$
iii) $a = 10299, m = 999.$	Solution: $10 = 10299 \div 999$; $309 = 10299 \div 999$
iv) $a = 123456, m = 1001.$	Solution: $123 = 123456 \div 1001$; $333 = 123456 \div 1001$

(b) Decide whether each of these integers is congruent to 5 modulo 17.

i) 80

Solution:

As We know that $a \equiv b \pmod{m}$ iff $\frac{a-b}{m}$.

Now $80 \not\equiv 5 \pmod{17}$ because $\frac{80-5}{17} = 4.41$.

ii) 103

As We know that $a \equiv b \pmod{m}$ iff $\frac{a-b}{m}$.

Now $103 \not\equiv 5 \pmod{17}$ because $\frac{103-5}{17} = 5.76$.

iii) -29

As We know that $a \equiv b \pmod{m}$ iff $\frac{a-b}{m}$.

Now $-29 \equiv 5 \pmod{17}$ because $\frac{-29-5}{17} = -2$.

iv) -122

As We know that $a \equiv b \pmod{m}$ iff $\frac{a-b}{m}$.

Now $-122 \not\equiv 5 \pmod{17}$ because $\frac{-122-5}{17} = -7.47$.

13. (a) Determine whether the integers in each of these sets are pairwise relatively prime.

i) 11, 15, 19

Solution: Yes

$\gcd(11, 15) = 1, \gcd(11, 19) = 1, \gcd(15, 19) = 1$

ii) 14, 15, 21

Solution: No

$\gcd(14, 15) = 1, \gcd(14, 21) = 7, \gcd(15, 21) = 3$

iii) 12, 17, 31, 37

Solution: Yes

$\gcd(12, 17) = 1, \gcd(12, 31) = 1, \gcd(12, 37) = 1, \gcd(17, 31) = 1, \gcd(17, 37) = 1, \gcd(31, 37) = 1$

iv) 7, 8, 9, 11

Solution: Yes

$\gcd(7, 8) = 1, \gcd(7, 9) = 1, \gcd(7, 11) = 1, \gcd(8, 9) = 1, \gcd(8, 11) = 1, \gcd(9, 11) = 1$

(b) Find the prime factorization of each of these integers.

i) 88

Solution: $88 = 2^3 * 11$

ii) 126

Solution: $126 = 2 * 3^2 * 7$

iii) 729

Solution: $729 = 3^6$

iv) 1001

Solution: $1001 = 7 * 13 * 11$

v) 1111

Solution: $1111 = 11 * 101$

vi) 909

Solution: $909 = 3^2 * 101$

14. Use the extended Euclidean algorithm to express $\gcd(144, 89)$ and $\gcd(1001, 100001)$ as a linear combination.

Solution:

$$\text{Gcd}(144,89) = (144)(34) + (89)(-55) = 1$$

$$\text{Gcd}(1001, 100001) = (10)(100001) + (-999)(1001) = 11$$

15. Solve each of these congruences using the modular inverses.

a) $55x \equiv 34 \pmod{89}$

Solution:

$$\text{Gcd}(55,89) = (55)(34) + (89)(-21) = 1$$

So, inverse $\bar{a} = 34$.

Multiply 34 both side

$$55 * 34 x \equiv 34 * 34 \pmod{89}$$

$$x \equiv 1156 \pmod{89} = 88.$$

b) $89x \equiv 2 \pmod{232}$

Solution:

$$\text{Gcd}(89,232) = (73)(89) + (232)(-28) = 1$$

So, inverse $\bar{a} = 73$,

Multiply 73 both side

$$89 * 73 x \equiv 2 * 73 \pmod{232}$$

$$x \equiv 146 \pmod{232} = 146.$$

16. (a) Use the construction in the proof of the Chinese remainder theorem to find all solutions to the system of congruences.

i) $x \equiv 1 \pmod{5}$, $x \equiv 2 \pmod{6}$, and $x \equiv 3 \pmod{7}$.

Solution:

We will follow the notation used in the proof of the Chinese remainder theorem.

$$\text{We have } m = m_1 * m_2 * m_3 = 5 * 6 * 7 = 210.$$

$$M_1 = 210/5 = 42, M_2 = 210/6 = 35, \text{ and } M_3 = 210/7 = 30$$

Also, by simple inspection we see that:

$$y_1 = 3 \text{ is an inverse for } M_1 = 42 \text{ modulo } 5, \quad y_2 = 5 \text{ is an inverse for } M_2 = 35 \text{ modulo } 6 \text{ and}$$

$$y_3 = 4 \text{ is an inverse for } M_3 = 30 \text{ modulo } 7.$$

The solutions to the system are then all numbers x such that

$$x = (a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3) \pmod{m} = ((1 * 42 * 3) + (2 * 35 * 5) + (3 * 30 * 4)) \pmod{210} \\ = 836 \pmod{210} = 206.$$

ii) $x \equiv 1 \pmod{2}$, $x \equiv 2 \pmod{3}$, $x \equiv 3 \pmod{5}$, and $x \equiv 4 \pmod{11}$.

Solution:

We will follow the notation used in the proof of the Chinese remainder theorem.

$$\text{We have } m = m_1 * m_2 * m_3 * m_4 = 2 * 3 * 5 * 11 = 330.$$

$$M_1 = 330/2 = 165, M_2 = 330/3 = 110, M_3 = 330/5 = 66 \text{ and } M_4 = 330/11 = 30$$

Also, by simple inspection we see that:

$$y_1 = 1 \text{ is an inverse for } M_1 = 165 \text{ modulo } 2, \quad y_2 = 2 \text{ is an inverse for } M_2 = 110 \text{ modulo } 3,$$

$$y_3 = 1 \text{ is an inverse for } M_3 = 66 \text{ modulo } 5 \text{ and } y_4 = 7 \text{ is an inverse for } M_4 = 30 \text{ modulo } 11.$$

The solutions to the system are then all numbers x such that

$$x = (a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 + a_4 M_4 y_4) \pmod{m} \\ = ((1 * 165 * 1) + (2 * 110 * 2) + (3 * 66 * 1) + (4 * 30 * 7)) \pmod{330} = 1643 \pmod{330} = 323.$$

(b) An old man goes to market and a camel step on his basket and crushes the oranges. The camel rider offers to pay for the damages and asks him how many oranges he had brought. He does not

remember the exact number, but when he had taken them out five at a time, there were 3 oranges left. When he took them six at a time, there were also three oranges left, when he had taken them out seven at a time, there was only one orange was left and when he had taken them out eleven at a time, there was no orange left. What is the number of oranges he could have had?

Solution:

We will follow the notation used in the proof of the Chinese remainder theorem.

We have $m = m_1 * m_2 * m_3 * m_4 = 2310$.

Also, by simple inspection we see that:

$y_1 = 3$ is an inverse for $M_1 = 462$ modulo 5,

$y_2 = 1$ is an inverse for $M_2 = 385$ modulo 6,

$y_3 = 1$ is an inverse for $M_3 = 330$ modulo 7 and

$y_4 = 1$ is an inverse for $M_4 = 210$ modulo 11.

The solutions to the system are then all numbers x such that

$$x = (a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3 + a_4 M_4 y_4) \bmod m$$

$$= (3 * 462 * 3) + (3 * 385 * 1) + (1 * 330 * 1) + (0 * 210 * 1) = 5643 \pmod{2310} = 1023.$$

He could have 1023 oranges.

17. Find an inverse of a modulo m for each of these pairs of relatively prime integers.

a) $a = 2, m = 17$

Solution:

$$\gcd(2, 17) = (1)(17) + (-8)(2) = 1$$

$$\text{So, } -8 + 17 = 9$$

Hence inverse, $\bar{a} = 9$.

b) $a = 34, m = 89$

Solution:

$$\gcd(34, 89) = (13)(89) + (-34)(34) = 1$$

$$\text{So, } -34 + 89 = 55$$

Hence inverse, $\bar{a} = 55$.

c) $a = 144, m = 233$

Solution:

$$\gcd(144, 233) = (89)(144) + (-55)(233) = 1$$

Hence inverse, $\bar{a} = 89$.

d) $a = 200, m = 1001$

Solution:

$$\gcd(200, 1001) = (1)(1001) + (-5)(200) = 1$$

$$\text{So, } -5 + 1001 = 996$$

Hence inverse, $\bar{a} = 996$.

18. (a) Encrypt the message STOP POLLUTION by translating the letters into numbers, applying the given encryption function, and then translating the numbers back into letters.

$$\text{i) } f(p) = (p + 4) \bmod 26$$

Solution:

S T O P P O L L U T I O N

18 19 14 15 15 14 11 11 20 19 8 14 13

After applying function:

22 23 18 19 19 18 15 15 24 23 12 18 17

W X S T T S P P Y X M S R will be encrypted message.

$$\text{ii) } f(p) = (p + 21) \bmod 26$$

Solution:

S T O P P O L L U T I O N
18 19 14 15 15 14 11 11 20 19 8 14 13

After applying function:

13 14 09 10 10 09 06 06 15 14 03 09 08

N O J K K J G G P O D J I will be encrypted message.

(b) Decrypt these messages encrypted using the Shift cipher. $f(p) = (p + 10) \bmod 26$.

i) CEBBOXNOB XYG

Solution:

“SURRENDER NOW” will be decrypted message.

ii) LO WI PBSOXN

Solution:

“BE MY FRIEND” will be decrypted message.

19. Use Fermat's little theorem to compute $5^{2003} \bmod 7$, $5^{2003} \bmod 11$, and $5^{2003} \bmod 13$.

Solution:

(i) $5^{2003} \bmod 7$

Solution: Since $5^6 = 1 \bmod 7$
 $= (5^6)^{333} \cdot 5^5 \bmod 7 = 5^5 \bmod 7 = 3.$

(ii) $5^{2003} \bmod 11$

Solution: Since $5^{10} = 1 \bmod 11$
 $= (5^{10})^{200} \cdot 5^3 \bmod 11 = 5^3 \bmod 11 = 4.$

(iii) $5^{2003} \bmod 13$

Solution: Since $5^{12} = 1 \bmod 13$
 $= (5^{12})^{166} \cdot 5^{11} \bmod 13 = 5^{11} \bmod 13 = 8.$

20. (a) Encrypt the message I LOVE DISCRETE MATHEMATICS by translating the letters into numbers, applying the Caesar Cipher Encryption function and then translating the numbers back into letters.

Solution:

The encrypted message will be “LORYH GLVFUHHW PDWKHPDWLFV “

(b) Decrypt these messages encrypted using the Caesar Cipher.

i) PLG WZR DVVLJQPHQW

Solution:

“MID TWO ASSIGNMENT” will be decrypted message.

ii) IDVW QXFHV XQLYHUVLWB

Solution:

“FAST NUCES UNIVERSITY “will be decrypted message.

21. (a) Which memory locations are assigned by the hashing function $h(k) = k \bmod 97$ to the records of insurance company customers with these Social Security numbers?

i) 034567981

Solution: $034567981 \bmod 97 = 91$

ii) 183211232

Solution: $183211232 \bmod 97 = 57$

iii) 220195744

Solution: $220195744 \bmod 97 = 21$

iv) 987255335

Solution: $987255335 \bmod 97 = 5$

(b) Which memory locations are assigned by the hashing function $h(k) = k \bmod 101$ to the records of insurance company customers with these Social Security numbers?

i) 104578690

Solution: $104578690 \bmod 101 = 58.$

ii) 432222187

Solution: $432222187 \bmod 101 = 60.$

iii) 372201919

Solution: $372201919 \bmod 101 = 32.$

iv) 501338753

Solution: $501338753 \bmod 101 = 3.$

22. What sequence of pseudorandom numbers is generated using the linear congruential generator?

$x_{n+1} = (4x_n + 1) \bmod 7$ with seed $x_0 = 3$?

Solution:

$X_1 = (4 * 3 + 1) \bmod 7 = 6.$

$X_2 = (4 * 6 + 1) \bmod 7 = 4.$

$X_3 = (4 * 4 + 1) \bmod 7 = 3.$

$X_4 = (4 * 3 + 1) \bmod 7 = 6.$

$X_5 = (4 * 6 + 1) \bmod 7 = 4$

Sequence: 6,4,3,6, 4,.....

23. (a) Determine the check digit for the UPCs that have these initial 11 digits.

i) 73232184434

Solution:

$$7*3 + 3 + 2*3 + 3 + 2*3 + 1 + 8*3 + 4 + 4*3 + 3 + 4*3 + x_{12} = 0 \bmod 10$$

$$21 + 3 + 6 + 3 + 6 + 1 + 24 + 4 + 12 + 3 + 12 + x_{12} = 0 \bmod 10$$

$$95 + x_{12} = 0 \bmod 10$$

Check digit is $x_{12} = 5.$

ii) 63623991346

Solution:

$$6*3 + 3 + 6*3 + 2 + 3*3 + 9 + 9*3 + 1 + 3*3 + 4 + 6*3 + x_{12} = 0 \bmod 10$$

$$18 + 3 + 18 + 2 + 9 + 9 + 27 + 1 + 9 + 4 + 18 + x_{12} = 0 \bmod 10$$

$$118 + x_{12} = 0 \bmod 10$$

Check digit is $x_{12} = 2.$

(b) Determine whether each of the strings of 12 digits is a valid UPC code.

i) 036000291452

Solution:

$$\begin{aligned}
0 \cdot 3 + 3 + 6 \cdot 3 + 0 + 0 \cdot 3 + 0 + 2 \cdot 3 + 9 + 1 \cdot 3 + 4 + 5 \cdot 3 + 2 &= 0 \pmod{10} \\
0 + 3 + 18 + 0 + 0 + 0 + 6 + 9 + 3 + 4 + 15 + 2 &= 0 \pmod{10} \\
60 &\equiv 0 \pmod{10}
\end{aligned}$$

It's a valid UPC code.

ii) 012345678903

Solution:

$$\begin{aligned}
0 \cdot 3 + 1 + 2 \cdot 3 + 3 + 4 \cdot 3 + 5 + 6 \cdot 3 + 7 + 8 \cdot 3 + 9 + 0 \cdot 3 + 3 &= 0 \pmod{10} \\
0 + 1 + 6 + 3 + 12 + 5 + 18 + 7 + 24 + 9 + 0 + 3 &= 0 \pmod{10} \\
88 &\not\equiv 0 \pmod{10}
\end{aligned}$$

It's not a valid UPC code.

24. (a) The first nine digits of the ISBN-10 of the European version of the fifth edition of this book are 0-07-119881. What is the check digit for that book?

Solution:

$$\begin{aligned}
1 \cdot 0 + 2 \cdot 0 + 3 \cdot 7 + 4 \cdot 1 + 5 \cdot 1 + 6 \cdot 9 + 7 \cdot 8 + 8 \cdot 8 + 9 \cdot 1 + x_{10} &= 0 \pmod{11} \\
0 + 0 + 21 + 4 + 5 + 54 + 56 + 64 + 9 + x_{10} &= 0 \pmod{11} \\
213 + x_{10} &= 0 \pmod{11}
\end{aligned}$$

Check digit, $x_{10} = 4$.

- (b) The ISBN-10 of the sixth edition of Elementary Number Theory and Its Applications is 0-321-500Q1-8, where Q is a digit. Find the value of Q.

Solution:

$$\begin{aligned}
x_{10} &= 1 \cdot 0 + 2 \cdot 3 + 3 \cdot 2 + 4 \cdot 1 + 5 \cdot 5 + 6 \cdot 0 + 7 \cdot 0 + 8 \cdot Q + 9 \cdot 1 \pmod{11} \\
&= 0 + 6 + 6 + 4 + 25 + 0 + 0 + 8Q + 9 \pmod{11} \\
&= 8Q + 50 \pmod{11}
\end{aligned}$$

The check digit is known to be 8.

$$8Q + 50 \pmod{11} = 8$$

Since $50 \pmod{11} = 6$

$$8Q + 6 \pmod{11} = 8$$

Subtract 6 from each side of the equation:

$$8Q \pmod{11} = 2$$

Since the inverse of $8 \pmod{11}$ is $7 \pmod{11}$, we should multiply both sides of the equation by 7:

$$\begin{aligned}
7 \cdot 8Q \pmod{11} &= 7 \cdot 2 \pmod{11} \\
56Q \pmod{11} &= 14 \pmod{11} \\
Q \pmod{11} &= 3
\end{aligned}$$

Since Q is a digit (between 0 and 9), Q then has to be equal to 3.

25. Encrypt the message ATTACK using the RSA system with $n = 43 \cdot 59$ and $e = 13$, translating each letter into integers and grouping together pairs of integers.

Solution:

A	T	T	A	C	K
00	19	19	00	02	10

- $n = 43 \cdot 59 = 2537$
- $k = (43 - 1)(59 - 1) = 2436$
- $e = 13$

Encryption Function: $C = M^e \pmod{n}$

$$C = 0019^{13} \pmod{2537}$$

$$C = 1900^{13} \pmod{2537}$$

$$C = 0210^{13} \pmod{2537}$$

26. (a) Find the first five terms of the sequence for each of the following general terms where $n > 0$.

(i) $2^n - 1$

Solution:

1,2,4,8,16 are the first five terms of the given sequence.

(ii) $10 - \frac{3}{2}n$

Solution:

$\frac{17}{2}, 7, \frac{11}{2}, 4, \frac{5}{2}$ are the first five terms.

(iii) $\frac{(-1)^n}{n^2}$

Solution:

$-1, \frac{1}{4}, -\frac{1}{9}, \frac{1}{16}, -\frac{1}{25}$ are the first five terms.

(iv) $\frac{3n+4}{2n-1}$

Solution: $7, \frac{10}{3}, \frac{13}{5}, \frac{16}{7}, \frac{19}{9}$ are the first five terms.

(b) Identify the following Sequence as Arithmetic or Geometric Sequence then find the indicated term.

(i) -15, -22, -29, -36,; 11th term.

Solution:

Here common difference (d) = -7

$$T_n = a + (n - 1)d; \quad T_{11} = -15 + (11 - 1)(-7) = -85$$

(ii) a - 42b, a - 39b, a - 36b, a - 33b,; 15th term.

Solution:

Here common difference (d) = 3b

$$T_n = a + (n - 1)d; \quad T_{15} = a - 42b + (15 - 1)(3b) = a$$

(iii) $4, 3, \frac{9}{4}, \dots$; 17th term

Solution:

Here common ratio (r) = $\frac{3}{4}$

$$T_n = ar^{n-1}; \quad T_{17} = 4\left(\frac{3}{4}\right)^{17-1} = \frac{3^{16}}{4^{15}}$$

(iv) 32, 16, 8,; 9th term

Solution:

Here common ratio (r) = $\frac{1}{2}$

$$T_n = ar^{n-1}; \quad T_{17} = 32\left(\frac{1}{2}\right)^{9-1} = \frac{1}{8}$$

27. (a) Find the G.P in which:

(i) $T_3 = 10$ and $T_5 = 2\frac{1}{2}$

Solution:

Since $T_n = ar^{n-1}$

$$T_3 = ar^2 = 10 \text{ ----(i)} \quad T_5 = ar^4 = \frac{5}{2} \text{ ----(ii)}$$

Now, dividing (ii) by dividing (i), we get $r = \pm \frac{1}{2}$ and putting it in (i) we get a = 40.

Now the required G.P is $40, 20, 10, 5, \frac{5}{2}, \dots$ OR $40, -20, 10, -5, \frac{5}{2}, \dots$

(ii) $T_5 = 8$ and $T_8 = -\frac{64}{27}$

Solution:

Since $T_n = ar^{n-1}$

$$T_5 = ar^4 = 8 \text{ ----(i)} \quad T_8 = ar^7 = -\frac{64}{27} \text{ ----(ii)}$$

Now, dividing (ii) by dividing (i) we get $r = -\frac{2}{3}$ and putting it in (i) we get $a = \frac{81}{2}$.

Now the required G.P is $\frac{81}{2}, -27, 18, -12, 8, \dots$

(b) Find the A.P in which:

$$(i) T_4 = 7 \text{ and } T_{16} = 31$$

Solution:

$$\text{Since } T_n = a + (n-1)d;$$

$$T_4 = a + 3d = 7 \text{(i)} \quad T_{16} = a + 15d = 31 \text{(ii)}$$

Now subtracting (ii) from (i), we get $d = 2$ and putting it in (i) we get $a = 1$.

Now the required A.P is $1, 3, 5, 7, 9, 11, \dots$

$$(ii) T_5 = 86 \text{ and } T_{10} = 146$$

Solution:

$$\text{Since } T_n = a + (n-1)d;$$

$$T_5 = a + 4d = 86 \text{(i)} \quad T_{10} = a + 9d = 146 \text{(ii)}$$

Now subtracting (ii) from (i), we get $d = 12$ and putting it in (i) we get $a = 38$.

Now the required A.P is $38, 50, 62, 74, 86, \dots$

28. (a) How many numbers are there between 256 and 789 that are divisible by 7. Also find their sum.

Solution:

First, we find the A.P with the common difference (d)= 7

259, 266, 273, 280, , 784

$$\text{Since } T_n = a + (n-1)d;$$

$$784 = 259 + (n-1)(7);$$

$$n = 76.$$

$$\text{Now for Sum; } S_n = \frac{n}{2} [2a + (n-1)d];$$

$$S_{76} = \frac{76}{2} [2(259) + (76-1)(7)] = 39,634.$$

(b) Find the sum to n terms of an A.P whose first term is $\frac{1}{n}$ and the last term is $\frac{n^2-n+1}{n}$.

Solution:

$$\text{Since, } S_n = \frac{n}{2} [2a + (n-1)d] \text{ ---- (i)}$$

1st we have to find "d"

$$\text{Now, } T_n = a + (n-1)d$$

$$\frac{n^2 - n + 1}{n} = \frac{1}{n} + (n-1)d$$

Finally, $d = 1$. Hence putting it in we get,

$$S_n = \frac{n^2 - n + 2}{2}.$$

29. (a) Use summation notation to express the sum of the first 100 terms of the sequence $\{a_j\}$, where $a_j = \frac{1}{j}$ for $j = 1, 2, 3, \dots$

Solution:

The lower limit for the index of summation is 1, and the upper limit is 100. We write this sum as $\sum_{j=1}^{100} \frac{1}{j}$.

(b) What is the value of:

$$(i) \sum_{k=4}^8 (-1)^k.$$

Solution:

$$\begin{aligned} &= (-1)^4 + (-1)^5 + (-1)^6 + (-1)^7 + (-1)^8 \\ &= 1 + (-1) + 1 + (-1) + 1 = 1. \end{aligned}$$

$$(ii) \sum_{j=1}^5 (j)^2.$$

Solution:

$$\begin{aligned} &= 1^2 + 2^2 + 3^2 + 4^2 + 5^2 \\ &= 1 + 4 + 9 + 16 + 25 = 55. \end{aligned}$$

30. Find the first six terms of the sequence defined by each of these recurrence relations and initial conditions.

a) $a_n = -2a_{n-1}$, $a_0 = -1$

Solution:

$$\begin{aligned} a_0 &= -1 \\ a_1 &= -2a_0 = -2(-1) = 2 \\ a_2 &= -2a_1 = -2(2) = -4 \\ a_3 &= -2a_2 = -2(-4) = 8 \\ a_4 &= -2a_3 = -2(8) = -16 \\ a_5 &= -2a_4 = -2(-16) = 32 \end{aligned}$$

b) $a_n = a_{n-1} - a_{n-2}$, $a_0 = 2$, $a_1 = -1$

Solution:

$$\begin{aligned} a_0 &= 2 \\ a_1 &= -1 \\ a_2 &= a_1 - a_0 = -1 - 2 = -3 \\ a_3 &= a_2 - a_1 = -3 - (-1) = -2 \\ a_4 &= a_3 - a_2 = -2 - (-3) = 1 \\ a_5 &= a_4 - a_3 = 1 - (-2) = 3 \end{aligned}$$

c) $a_n = 3a_{n-1}^2$, $a_0 = 1$

Solution:

$$\begin{aligned} a_0 &= 1 \\ a_1 &= 3a_0^2 = 3(1^2) = 3 \\ a_2 &= 3a_1^2 = 3(3^2) = 3(9) = 27 \\ a_3 &= 3a_2^2 = 3(27^2) = 3(729) = 2187 \\ a_4 &= 3a_3^2 = 3(2187^2) = 3(4782969) = 14348907 \\ a_5 &= 3a_4^2 = 3(14348907^2) = 3(205891132094649) = 617673396283947 \end{aligned}$$

d) $a_n = na_{n-1} + a_{n-2}^2$, $a_0 = -1$, $a_1 = 0$

Solution:

$$a_0 = -1$$

$$a_1 = 0$$

$$a_2 = 2a_1 + a_0^2 = 2(0) + (-1)^2 = 0 + 1 = 1$$

$$a_3 = 3a_2 + a_1^2 = 3(1) + 0^2 = 3 + 0 = 3$$

$$a_4 = 4a_3 + a_2^2 = 4(3) + 1^2 = 12 + 1 = 13$$

$$a_5 = 5a_4 + a_3^2 = 5(13) + 3^2 = 65 + 9 = 74$$

31. Prove the statement: There is an integer $n > 5$ such that $2^n - 1$ is prime.

Solution: Here we are asked to show a single integer for which $2^n - 1$ is prime. First of all we will check the integers from 1 and check whether the answer is prime or not by putting these values in $2^n - 1$. When we got the answer is prime then we will stop our process of checking the integers and we note that,

Let $n = 7$, then

$$2^n - 1 = 2^7 - 1 = 128 - 1 = 127$$

and we know that 127 is prime.

(b) Prove that for any integer a and any prime number p , if $p \mid a$, $p \nmid (a + 1)$.

Solution:

Suppose there exists an integer a and a prime number p such that $p \mid a$ and $p \mid (a+1)$.

Then by definition of divisibility there exist integer r and s so that

$$a = p \cdot r \text{ and } a + 1 = p \cdot s$$

It follows that

$$\begin{aligned} 1 &= (a + 1) - a \\ &= p \cdot s - p \cdot r \\ &= p \cdot (s - r) \quad \text{where } s - r \in \mathbb{Z} \end{aligned}$$

This implies $p \mid 1$.

But the only integer divisors of 1 are 1 and -1 and since p is prime $p > 1$. This is a contradiction. Hence the supposition is false, and the given statement is true.

32. (a) Prove the statement: There are real numbers a and b such that $\sqrt{(a + b)} = \sqrt{a} + \sqrt{b}$.

Solution:

$$\text{Let } \sqrt{(a + b)} = \sqrt{a} + \sqrt{b}$$

Squaring, we get $a + b = a + b + 2\sqrt{a}\sqrt{b}$

$$\Rightarrow 0 = 2\sqrt{a}\sqrt{b} \quad \text{cancelling } a + b$$

$$\Rightarrow 0 = 2\sqrt{ab}$$

$$\Rightarrow 0 = ab \quad \text{squaring}$$

$$\Rightarrow \text{either } a = 0 \text{ or } b = 0$$

It means that if we want to find out the integers which satisfy the given condition then one of them must be zero. Hence if we let $a = 0$ and $b = 3$ then

$$\text{R.H.S} = \sqrt{(a + b)} = \sqrt{0 + 3} = \sqrt{3}$$

Now,

$$\text{L.H.S} = \sqrt{0} + \sqrt{3} = \sqrt{3}$$

From above it quite clear that the given condition is satisfied if we take $a=0$ and $b=3$.

(b) Prove that if $|x| > 1$ then $x > 1$ or $x < -1$ for all $x \in \mathbb{R}$.

Solution:

The contrapositive statement is:

if $x \leq 1$ and $x \geq -1$ then $|x| \leq 1$ for $x \in \mathbb{R}$.

Suppose that $x \leq 1$ and $x \geq -1$

$\Rightarrow x \leq 1$ and $x \geq -1$

$\Rightarrow -1 \leq x \leq 1$

and so

$|x| \leq 1$

Equivalently $|x| > 1$.

33. (a) Find a counter example to the proposition: For every prime number n , $n + 2$ is prime.

SOLUTION:

Let the prime number n be 7, then

$$n + 2 = 7 + 2 = 9$$

which is not prime.

(b) Show that the set of prime numbers is infinite.

Solution:

Suppose the set of prime numbers is finite.

Then, all the prime numbers can be listed, say, in ascending order:

$$p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, \dots, p_n$$

Consider the integer

$$N = p_1 \cdot p_2 \cdot p_3 \cdot \dots \cdot p_n + 1$$

Then $N > 1$. Since any integer greater than 1 is divisible by some prime number p , therefore $p \mid N$.

Also since p is prime, p must equal one of the prime numbers

$$p_1, p_2, p_3, \dots, p_n.$$

Thus

$$p \mid (p_1 \cdot p_2 \cdot p_3 \cdot \dots \cdot p_n)$$

But then

$$p \nmid (p_1 \cdot p_2 \cdot p_3 \cdot \dots \cdot p_n + 1)$$

$$\text{So } p \nmid N$$

Thus $p \mid N$ and $p \nmid N$, which is a contradiction.

Hence the supposition is false and the theorem is true.

34. (a) Prove by contradiction method, the statement: If n and m are odd integers, then $n + m$ is an even integer.

Solution:

Suppose n and m are odd and $n + m$ is not even (odd i.e by taking contradiction).

Now $n = 2p + 1$ for some integer p

and $m = 2q + 1$ for some integer q

Hence $n + m = (2p + 1) + (2q + 1)$

$$= 2p + 2q + 2 = 2 \cdot (p + q + 1)$$

which is even, contradicting the assumption that $n + m$ is odd.

(b) Prove the statement by contraposition: For all integers m and n , if $m + n$ is even then m and n are both even or m and n are both odd.

Solution:

“For all integers m and n , if m and n are not both even and m and n are not both odd, then $m + n$ is not even.”

Or more simply,

“For all integers m and n , if one of m and n is even and the other is odd, then $m + n$ is odd”

Suppose m is even and n is odd. Then

$$\begin{array}{ll} m = 2p & \text{for some integer } p \\ \text{and } n = 2q + 1 & \text{for some integer } q \\ \text{Now } m + n = (2p) + (2q + 1) & \\ = 2 \cdot (p + q) + 1 & \\ = 2 \cdot r + 1 & \text{where } r = p + q \text{ is an integer} \end{array}$$

Hence $m + n$ is odd.

Similarly, taking m as odd and n even, we again arrive at the result that $m + n$ is odd.

Thus, the contrapositive statement is true. Since an implication is logically equivalent to its contrapositive so the given implication is true.

35. Prove by contradiction that $6 - 7\sqrt{2}$ is irrational.

Solution:

Suppose $6 - 7\sqrt{2}$ is rational.

Then by definition of rational,

$$6 - 7\sqrt{2} = \frac{a}{b}$$

for some integers a and b with $b \neq 0$.

Now consider,

$$\begin{aligned} 7\sqrt{2} &= 6 - \frac{a}{b} \\ \Rightarrow 7\sqrt{2} &= \frac{6b - a}{b} \\ \Rightarrow \sqrt{2} &= \frac{6b - a}{7b} \end{aligned}$$

Since a and b are integers, so are $6b - a$ and $7b$ and $7b \neq 0$;

hence $\sqrt{2}$ is a quotient of the two integers $6b - a$ and $7b$ with $7b \neq 0$.

Accordingly, $\sqrt{2}$ is rational (by definition of rational).

This contradicts the fact because $\sqrt{2}$ is irrational.

Hence our supposition is false and so $6 - 7\sqrt{2}$ is irrational.

(b) Prove by contradiction that $\sqrt{2} + \sqrt{3}$ is irrational.

Solution:

Suppose $\sqrt{2} + \sqrt{3}$ is rational. Then, by definition of rational, there exists integers a and b with $b \neq 0$ such that

$$\sqrt{2} + \sqrt{3} = \frac{a}{b}$$

Squaring both sides, we get

$$\begin{aligned} 2 + 3 + 2\sqrt{2}\sqrt{3} &= \frac{a^2}{b^2} \\ \Rightarrow 2\sqrt{2 \times 3} &= \frac{a^2}{b^2} - 5 \\ \Rightarrow 2\sqrt{6} &= \frac{a^2 - 5b^2}{b^2} \\ \Rightarrow \sqrt{6} &= \frac{a^2 - 5b^2}{2b^2} \end{aligned}$$

Since a and b are integers, so are therefore $a^2 - 5b^2$ and $2b^2$ with $2b^2 \neq 0$. Hence $\sqrt{6}$ is the quotient of two integers $a^2 - 5b^2$ and $2b^2$ with $2b^2 \neq 0$. Accordingly, $\sqrt{6}$ is rational. But this is a contradiction, since $\sqrt{6}$ is not rational. Hence our supposition is false and so $\sqrt{2} + \sqrt{3}$ is irrational.

REMARK:

The sum of two irrational numbers need not be irrational in general for

$$(6 - 7\sqrt{2}) + (6 + 7\sqrt{2}) = 6 + 6 = 12$$

which is rational.

36. (a) By mathematical induction, prove that following is true for all positive integral values of n.

(a) $1^2 + 2^2 + 3^2 + \dots + n^2 = \frac{n(n+1)(2n+1)}{6}$

SOLUTION:

Let P(n) denotes the given equation

1. Basis step:

P(1) is true
For n = 1
L.H.S of P(1) = $1^2 = 1$

$$\begin{aligned} \text{R.H.S of P(1)} &= \frac{1(1+1)(2(1)+1)}{6} \\ &= \frac{(1)(2)(3)}{6} = \frac{6}{6} = 1 \end{aligned}$$

So L.H.S = R.H.S of P(1). Hence P(1) is true

2. Inductive Step:

Suppose P(k) is true for some integer $k \geq 1$;

$$1^2 + 2^2 + 3^2 + \dots + k^2 = \frac{k(k+1)(2k+1)}{6} \quad \dots\dots\dots(1)$$

To prove P(k+1) is true; i.e.;

$$1^2 + 2^2 + 3^2 + \dots + (k+1)^2 = \frac{(k+1)(k+1+1)(2(k+1)+1)}{6} \quad \dots(2)$$

Consider LHS of above equation (2)

$$\begin{aligned}
 1^2 + 2^2 + 3^2 + \dots + (k+1)^2 &= 1^2 + 2^2 + 3^2 + \dots + k^2 + (k+1)^2 \\
 &= \frac{k(k+1)(2k+1)}{6} + (k+1)^2 \\
 &= (k+1) \left[\frac{k(2k+1)}{6} + (k+1) \right] \\
 &= (k+1) \left[\frac{k(2k+1) + 6(k+1)}{6} \right] \\
 &= (k+1) \left[\frac{2k^2 + k + 6k + 6}{6} \right] \\
 &= \frac{(k+1)(2k^2 + 7k + 6)}{6} \\
 &= \frac{(k+1)(k+2)(2k+3)}{6} \\
 &= \frac{(k+1)(k+1+1)(2(k+1)+1)}{6}
 \end{aligned}$$

(b) $1+2+2^2 + \dots + 2^n = 2^{n+1} - 1$ for all integers $n \geq 0$

SOLUTION:

Let $P(n): 1 + 2 + 2^2 + \dots + 2^n = 2^{n+1} - 1$

1. Basis Step:

$P(0)$ is true.

For $n = 0$

L.H.S of $P(0) = 1$

R.H.S of $P(0) = 2^{0+1} - 1 = 2 - 1 = 1$

Hence $P(0)$ is true.

2. Inductive Step:

Suppose $P(k)$ is true for some integer $k \geq 0$; i.e.,

$$1+2+2^2+\dots+2^k = 2^{k+1} - 1 \dots\dots\dots(1)$$

To prove $P(k+1)$ is true, i.e.,

$$1+2+2^2+\dots+2^{k+1} = 2^{k+1+1} - 1 \dots\dots\dots(2)$$

Consider LHS of equation (2)

$$\begin{aligned}
 1+2+2^2+\dots+2^{k+1} &= (1+2+2^2+\dots+2^k) + 2^{k+1} \\
 &= (2^{k+1} - 1) + 2^{k+1} \\
 &= 2 \cdot 2^{k+1} - 1 \\
 &= 2^{k+1+1} - 1 = \text{R.H.S of (2)}
 \end{aligned}$$

Hence $P(k+1)$ is true and consequently by mathematical induction the given propositional function is true for all integers $n \geq 0$.

(c) $1^3 + 2^3 + 3^3 + \dots + n^3 = \frac{1}{4} n^2(n+1)^2$

Solution:

1. Show it is true for $n=1$

$$1^3 = \frac{1}{4} \times 1^2 \times 2^2 \text{ is True}$$

2. Assume it is true for $n=k$

$$1^3 + 2^3 + 3^3 + \dots + k^3 = \frac{1}{4} k^2(k+1)^2 \text{ is True (An assumption!)}$$

Now, prove it is true for " $k+1$ "

$$1^3 + 2^3 + 3^3 + \dots + (k+1)^3 = \frac{1}{4} (k+1)^2(k+2)^2$$

We know that $1^3 + 2^3 + 3^3 + \dots + k^3 = \frac{1}{4}k^2(k+1)^2$ (the assumption above), so we can do a replacement for all but the last term:

$$\frac{1}{4}k^2(k+1)^2 + (k+1)^3 = \frac{1}{4}(k+1)^2(k+2)^2$$

Multiply all terms by 4:

$$k^2(k+1)^2 + 4(k+1)^3 = (k+1)^2(k+2)^2$$

All terms have a common factor $(k+1)^2$, so it can be canceled:

$$k^2 + 4(k+1) = (k+2)^2$$

And simplify:

$$k^2 + 4k + 4 = k^2 + 4k + 4$$

They are the same! So it is true.

So:

$$1^3 + 2^3 + 3^3 + \dots + (k+1)^3 = \frac{1}{4}(k+1)^2(k+2)^2 \text{ is True}$$

37. As we have discussed, the practical application of all the topics in the class. Now you are required to submit at least two real world applications of the following topics.

(a) Propositional Logic

State Space Search:

State-space search is the issue of testing whether a state in a change framework is reachable from at least one starting states. Change frameworks in the most fundamental cases can be identified with diagrams, and the state-space search issue for this situation is the s-t-reachability issue in charts.

Old style propositional rationale has been proposed as one response for state-space look issues for amazingly gigantic charts, due to the possibility of addressing and pondering colossal amounts of states with (by and large little) recipes.

EXAMPLE:

$A \wedge B$ represents the set {1100, 1101, 1110, 1111} and $A \vee B$ represents the set {0100, 0101, 0110, 0111, 1000, 1001, 1010, 1011, 1100, 1101, 1110, 1111}.

Questions about the relations between sets represented as formulas can be reduced to the basic logical concepts we already know, namely logical consequence, satisfiability, and validity.

1. "Is ϕ satisfiable?" corresponds to "Is the set represented by ϕ non-empty?"
2. $\phi \models \alpha$ corresponds to "Is the set represented by ϕ a subset of the set represented by α ?"
3. "Is ϕ valid?" corresponds to "Is the set represented by ϕ the universal set?"

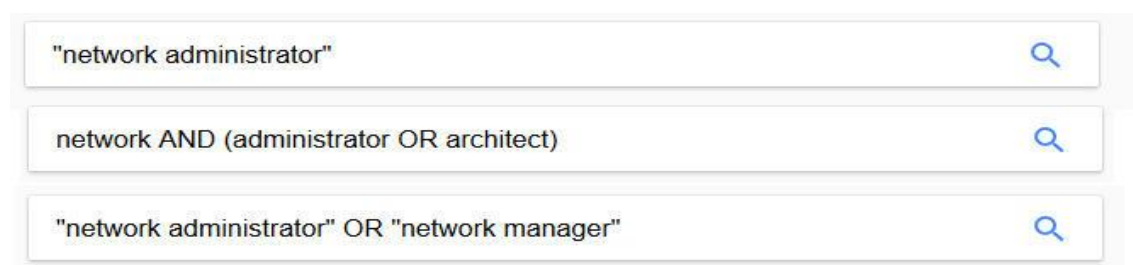
These connections allow using propositional formulas as a data structure in some applications in which conventional enumerative data structures for sets are not suitable because of the astronomic number of states. For example, if there are 100 state variables, then any formula consisting of just one atomic proposition represents a set of $2^{99} = 633825300114114700748351602688$ bit-vectors, which would require 7493989779944505344 TB in an explicit enumerative representation if each of the 100-bit vectors was represented with 13 bytes (wasting only 4 bits in the 13th byte.)

Boolean Searches:

Web indexes utilizing Boolean hunts utilize consistent connectives.

- AND requires records coordinate the two terms
- OR returns records that coordinate either of the terms
- NOT (or now and then AND NOT) rejects a term

Basic Boolean search commands (quotes, AND and OR) are supported in Google search, however Google defaults to AND searches automatically, so you don't need to enter AND into the search box. Google search uses additional symbols and words to refine searches such as "site:" to search a specific site or domain or use \$ in front of a number to search for a price.



The image shows three Google search boxes stacked vertically. The first box contains the text "network administrator" followed by a magnifying glass icon. The second box contains the text "network AND (administrator OR architect)" followed by a magnifying glass icon. The third box contains the text "\"network administrator\" OR \"network manager\"" followed by a magnifying glass icon.

(b) Predicates and quantifiers

Man-Made Intelligence:

Man-made consciousness is worried about information portrayal and rationales. Data Representation is a sub zone of Artificial Intelligence stressed over getting, organizing, and executing techniques for addressing information in PCs, and to surmise new information reliant on the addressed information. The predicate rationale is a piece of man-made brainpower which is relevant in the field of mechanical technology, medication and it is utilized in smart database so as to tackle some unpredictable issue.

EXAMPLE:

1. Mary loves everyone. [assuming D contains only humans]
 $\forall x \text{ love (Mary, x)}$
Note: No further parentheses are needed here, and according to the syntax on the handout, no further parentheses are possible. But "extra parentheses" are in general considered acceptable, and if you find them helpful, I have no objection. So I would also count as correct any of the following:
 $\forall x (\text{love (Mary, x)})$, $(\forall x \text{ love (Mary, x)})$, $(\forall x (\text{love (Mary, x)}))$

Computer infers new conclusions in the same way using predicate logics and quantifiers.

Legitimate inferences:

Predicate Logic can be utilized to check legitimacy of a deduced conclusion. Using predicate logic, we can validate inferences.

Consider these statements, of which the first three are premises and the fourth is a valid conclusion.

"All hummingbirds are richly colored."

“No large birds live on honey.”

“Birds that do not live on honey are dull in color.”

“Hummingbirds are small.”

Let $P(x)$, $Q(x)$, $R(x)$, and $S(x)$ be the statements “ x is a hummingbird,” “ x is large,” “ x lives on honey,” and “ x is richly colored,” respectively. Assuming that the domain consists of all birds, express the statements in the argument using quantifiers and $P(x)$, $Q(x)$, $R(x)$, and $S(x)$.

Solution: We can express the statements in the argument as

$\forall x(P(x) \rightarrow S(x)).$

$\neg \exists x(Q(x) \wedge R(x)).$

$\forall x(\neg R(x) \rightarrow \neg S(x)).$

$\forall x(P(x) \rightarrow \neg Q(x)).$

(c) Sets

Clusters:

Clusters are likely the most well-known assortment type. A cluster stores an arranged assortment of qualities. As I referenced before, the qualities put away in an exhibit are of a similar sort. Sets and exhibits share a few highlights for all intents and purpose. The two of them store an assortment of estimations of a similar kind. You can include and evacuate components if the set or cluster is variable in this way exhibit is inferred for the idea of set wherein each position has interesting worth simply like sets.

EXAMPLES:

Char array [6] = {'a', 'b', 'c', 'd', 'e', 'f'}

In sets, this can be represented in the following way:

{(0,a), (1,b), (2,c), (3,d), (4,e), (5,f)}

SQL:

SQL is a domain-specific language used in programming and designed for managing data held in a relational database management system, or for stream processing in a relational data stream management system.

EXAMPLE:

1. Union:
This set operator is used to combine the outputs of two or more queries into a single set of rows and columns having different records.
2. Union All:
This set operator is used to join the outputs of two or more queries into a single set of rows and columns without the removal of any duplicates.
3. Intersect:
This set operator is availed to retrieve the information which is common in both tables. The number of columns and data type must be same in intersect set operator.

(d) Functions

Functions in Physics:

Functions are frequently used in Physics and Mathematics.

EXAMPLE: You have given the velocity of rocket as 12000km/sec and the time required to reach the moon is 3 days. You have to compute the distance between Earth and Moon.

Formula: $S(t) = V \cdot t$

After changing the given information into SI units:

$S(259200) = 12000000 \cdot 259200$

$S(259200) = 3.1104 \times 10^{12}$ meters

Functions in Programming:

Functions is the essential part of learning PC writing computer programs is tied in with taking a contribution from the client then in the wake of experiencing some work restoring a worth simply like taking an area and delivering a range.

We can make our own, "User Defined Function".

EXAMPLES:

An example of user defined function in c++ is:

```
void Print()
{
    string name;
    cin >> name;
    cout << "Your Name is: " << name;
}
```

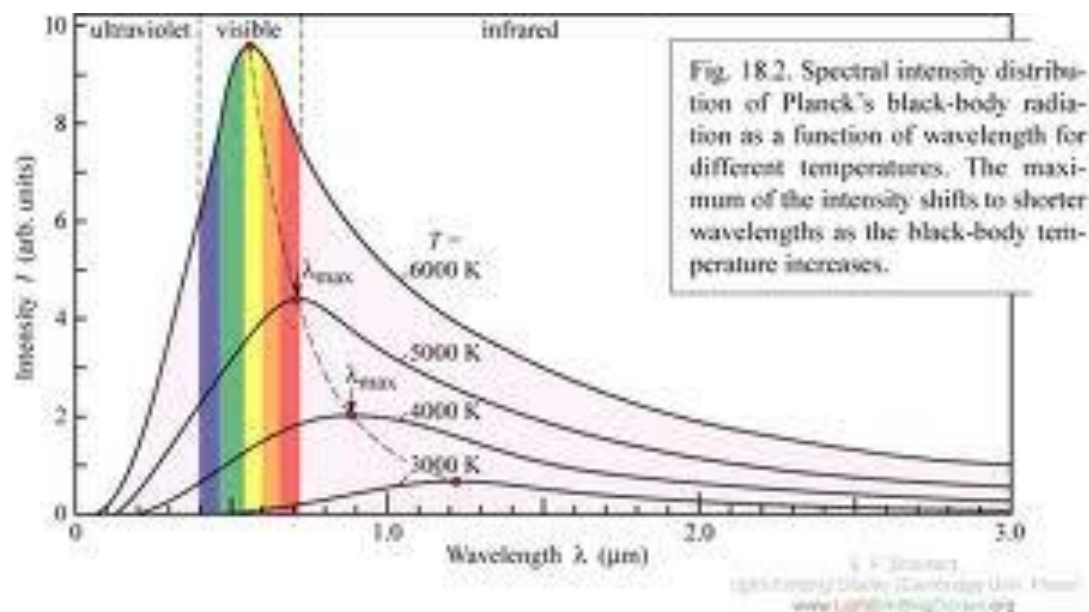

(e) Relations

Graphs:

In different fields of science diagrams are being plotted for telling the idea of relations between two things so chart is determined by plotting estimations of area (x-values) against range (y-values). A diagram can be looked as a method for deciphering relations.

EXAMPLES:

Here is the relation between frequency and wavelength showed by a graph:



Relations in real life:

Relations is used in real life in such ways that we cannot determine and notice all times.

EXAMPLE:

If someone has one gallon left in his fuel tank and he has to visit five places with this amount of fuel. So, with one gallon, he visits five places. So there is five outputs at one input.

(f) Sequence and Series

Sequence and series are widely used to in computer science, engineering, finance and economics etc to determine various possibilities of a certain situation or criteria to design, analyze, predict something or to build. For example, the interest portion of monthly payments made to pay off an automobile or home loan, and the list of maximum daily temperatures in one area for month are sequences.

Another application of sequence and series are the \$ sale or cost of more than one product. For example: if you go to a supermarket the prices of shirts are different and ~~are placed~~ ~~in a sequence of low to high cost.~~ the shirts are placed in a sequence like:

Rs 400

shirts,

Rs 500

shirts.

Rs 750

shirts

(g) Proof methods and Mathematical Induction

Proofs aren't just ways to show that the statements are true or valid. They help in proper understanding of rules, theorems, axioms and hypothesis. This application is frequently used in architecture, woodworking, or other physical construction projects. For instance, say you are building a sloped roof. If you know the height of the roof and the length for it to cover, you can use the Pythagoras Theorem to find the diagonal length of the roof's slope.

Another real life application of proofs are of programming. Computer science courses consists of proofs. For example of Solving problems in programming language proofs are extremely useful for demonstrating that you have properly solved the problem you are trying to solve.