Counting :

→ Counting problems arise throughout mathematics & Computer Science. Ex: we must count the successful outcomes of experiments & all the possible outcomes of these experiments to determine probability of discrete events.

⇒ we need to count the no. of operations used by an algorithm to study its Complexity.

Basic Counting Principles

Two basic counting principles are the product rule & the sum rule.

Product rule :

Suppose that a procedure can be broken down into a sequence of two tasks. If there are n_1 ways to do the first task & for each of these ways of doing the first task, there are n_2 ways to do the second task, then there are $n_1 n_2$ ways to do the procedure.

(a) The chairs of an auditorium are to be labeled with a letter & a +ve integer not exceeding 100. What is the largest no. of chairs that can be labeled differently?

A. The procedure of labelling a chair consists of two tasks.

1) Assigning one of the 26 letters
2) " " " 100 possible integers to the seat.

The product rule shows that

$26 \times 100 = 2600$ diff. ways that a chair can be labeled.

(a) How many diff license plates are available if each plate contains a sequence of three letters followed by three digits (and no sequences of letters are prohibited, even if they are obscene)?

Sol:- There are 26 choices for each of the three letters & ten choices for each of the 3-digits.

$\therefore$ $26.26.26.10.10.10 = 17,576,000$ possible license plates

Counting one-to-one functions

(a) How many one-to-one functions are there from the set with 'm'-elements to one with 'n'-elements?

Sol:- If $m > n$ it is not one-to-one.

Now let $m \leq n$ Suppose the elements are $a_1, a_2 \ldots a_m$

There 'n'-ways to choose from a_1

$(n-1)$ " " " a_2 ——

a_k —— $(n-k+1)$

$n(n-1)\ldots(n-m+1)$

Task of choosing an element in cartesian product.

$$|A_1 \times A_2 \times \cdots \times A_m| = |A_1| \cdot |A_2| \cdot \cdots |A_m|$$

Sum Rule:- If a task can be done either in one of n_1 ways or in one of n_2 ways, where none of the set of n_1 ways is same as any of the set of n_2 ways, then there are $n_1 + n_2$ ways to do the task.

(a) A student can choose a computer project from one of 3 lists. The three lists contain 23, 15 & 19 possible projects, respectively. No project is on more than one list. How many possible projects are there to choose from?

Sol:- The student can choose a project by selecting a project from the first list, second list, or the third list.

$\therefore$ The Sum rule $23+15+19 = 57$ ways to choose project.

The Sum rule can be phrased interms of sets as

$$|A_1 \cup A_2 \cup \cdots \cup A_m| = |A_1| + |A_2| + \cdots + |A_m|.$$

(a) Suppose that either a member of the mathematics faculty or a student who is a mathematics major is chosen as representative to a university committee. How many diff. choices are there for this representative if there are 37 members of mathematics faculty & 83 mathematics major & no one is both faculty member & student?

At 37 ways to choose mathematics faculty
83 " " " major

Choosing mathematics faculty is never the same as a student who is a mathematics major.
no one is both L I S.

By Sum rule 83+37 = 120 possible ways to pick this representative.

∴ More Complex Counting Problems:

(Q) Each user on a cp System has a password, which is six to eight characters long, where each character is an uppercase letter or digit. Each password must contain at least one digit. How many possible passwords are there?

At Let 'p' be the total no. of possible passwords.
Let P_6, P_7 & P_8 denote the no. of " " of length 6, 7 & 8 respectively.

→ 6×6

$36^6 - 26^6$

P_6 = no. of strings of uppercase letters & digits that are six character long including those with no digits

(and) Subtract from this the no. of strings with no digits

$P_6 = 36^6 - 26^6 = 1,867,866,560$

$P_7 = 36^7 - 26^7 = 70,332,353,920$

$P_8 = 36^8 - 26^8 = 2,612,282,842,880$

$P = P_6 + P_7 + P_8 = 2,684,483,063,360.$

(Q) Counting Internet Addresses:

In the Internet

How many diff IPV4 addresses are available for Computers on the Internet?

Bit number	0	1	2	3	4	8	16	24	31
class A	0	netId				hostId			
class B	1	0				netId	hostId		
class C	1	1	0			netId		hostId.	
class D	1	1	1	0		Multicast Address			
class E	1	1	1	1	0	Address.			

neither class D nor class E are assigned as the IP address of cp on the Internet

$x_A = 2^7 - 1$, net Ids

2^{24} - 2 host

$x_A = (2^7 - 1) \times (2^{24} - 2)$

$x_B = 2^{14}$ net Ids

$(2^{16} - 2)$ host Ids

$x_C = 2^{21}$ net Ids

$2^8 - 2 =$ host Ids.

$= (2^7 - 1)(2^{24} - 2) + (2^{14})(2^{16} - 2) + (2^{21})(2^8 - 2)$

The Inclusion & Exclusion Principle

Suppose that a task can be done in n_1 ways but that some of n_1 ways to do the task are same as some of the n_2 other way to do the task. In this situation we can't use the sum rule.

Adding the no. of ways to do the task in these 2-ways leads to an overcount.

→ To correctly count the no. of ways to do the 2 tasks, we add the no. of ways to do it in one ways + the no. of ways to do in the other way, & then subtract the no. of ways to do the task in a way that is both among the set of n_1 ways & set of n_2 ways called Principle of inclusion-exclusion.

$$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$$

② A cp company can receive 350

$|A_1| = 220, \quad |A_2| = 147 \quad |A_1 \cap A_2| = 51$

$\overline{A_1 \cup A_2} = ?$ $\quad |A_1 \cup A_2| = 350$

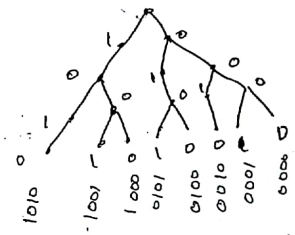
$|A_1 \cup A_2| = 220 + 147 - 51 = 316$

$|\overline{A_1 \cup A_2}| = 350 - 316 = 34$

Tree diagrams:

Counting problems can be solved using tree diagrams. We use trees in counting, we use a branch to represent each possible choice. We represent the possible outcomes by the leaves which are the endpoints of branches not having other branches starting at them

② How many bit strings of length four do not have two consecutive 1's?



② How many the integers between 1 to 400 inclusive

ⓐ Are divisible by 6?

$$\left\lfloor \frac{400}{6} \right\rfloor = 66$$

ⓑ not divisible by 6?

$400 - 66 = 334$

ⓒ divisible by 6 & 8

$$\left\lfloor \frac{400}{24} \right\rfloor = 16$$

ⓓ divisible by 6 or 8

$$|A_1 \cup A_2| = \left\lfloor \frac{400}{6} \right\rfloor + \left\lfloor \frac{400}{8} \right\rfloor - \left\lfloor \frac{400}{24} \right\rfloor$$

$= 100$

) How many integers the 100 to 999 are odd.

divisible by 2: $\left\lfloor \frac{999-100}{2} \right\rfloor = 449$

not divisible by 2: $899 - 449 = 450$

ⓐ How many the integers between 100 & 999 inclusive

ⓐ are divisible by 7?

$\left\lfloor \frac{999-100}{7} \right\rfloor =$

ⓑ are not divisible by 4?

$\left\lfloor \frac{999-100}{4} \right\rfloor = \left\lfloor \frac{899}{4} \right\rfloor = 224$

$899 - 224 = 675$

ⓒ are divisible by 3 or 4?

3 or $= \left\lfloor \frac{999-100}{3} \right\rfloor + \left\lfloor \frac{999-100}{4} \right\rfloor - \left\lfloor \frac{999-100}{3\times 4} \right\rfloor$

$= 299 + 224 - 74$

$= 449$

$899 - 449 = 450$

The Pigeonhole Principle:-

Def:- If 'k' is a the integer and k+1 or more objects are placed into k- boxes, then there is atleast one box containing two or more of the objects.

→ The Pigeonhole Principle is also called the "Dirichlet drawer principle"

⇒ A function 'f' from a set with 'k+1' or more elements to a set with 'k' elements is not one-to-one.

ⓐ Among any group of 367 people, there must be at least two with the same birthday, because, there are only 366 possible birthdays.

ⓑ In any group of 27 English words, there must be atleast two that begin with the same letter, because there are 26 letters in the English alphabet.

ⓒ How many students must be in a class to guarantee that at least two students receive the same score on the final exam, if the exam is graded on a scale from 0 to 100 points?

At There are 101 possible scores on the final.
The pigeon hole principle shows that among any 102 students there must be at least 2 students with the same score.

(a) The generalized Pigeonhole Principle

If N-objects are placed into k-boxes, then there is at least one box containing $\lceil N/k \rceil$ objects.

'r' → objects are placed in each k-box

$$\left\lceil \frac{N}{k} \right\rceil \geq r$$

for the smallest integer 'N'

with $\frac{N}{k} > r-1 \Rightarrow \boxed{N = k(r-1)+1}$ is the smallest integer satisfying the inequality $\left\lceil \frac{N}{k} \right\rceil \geq r$

(b) Among 100 people, how many are born in the same month?

$$\left\lceil \frac{100}{12} \right\rceil = 9$$

(c) What is the min. no. of students required in a discrete mathematics class to be sure that at least six will receive the same grade, if there are 5 possible grades. A, B, C, D, & F?

Atleast 6, $\left\lceil \frac{N}{5} \right\rceil = 6$, $N = 5 \cdot 5 + 1 = 26$

Elegant Appln of Pigeon hole Principle — The objects must be chosen from 15 to 30, placed in boxes must be chosen from 1 to 5

(a) During a month with 30 days, a baseball team plays atleast one game a day, but no more than 45 games. Show that there must be a period of some no of consecutive days during which the team must play exactly 14 games.

atleast one game a day, but no more than 45 games

Let a_j be the no. of games played on or before the j^{th} day of the month.

→ Then $a_1, a_2, \ldots, a_{30}$ is an increasing sequence of distinct +ve integers.

with $1 \leq a_j \leq 45$.

Moreover $a_1+14, a_2+14, \ldots, a_{30}+14$ is ''

with $15 \leq a_j+14 \leq 59$

The 60 +ve integers $a_1, a_2, \ldots, a_{30}, a_1+14, a_2+14, \ldots, a_{30}+14$ are all less than or equal to 59.

By pigeon hole principle two of these integers are equal. $\because$ a_j, $j = 1, 2, \ldots 30$

a_j+14 $j = 1, 2, \ldots 30$.

$\boxed{a_i = a_j + 14}$ $\therefore$ exactly 14 games are played from day $j+1$ to day i

Def: Every sequence of n^2+1 distinct real no's contain a subsequence of length $n+1$ i.e., either strictly increasing or strictly decreasing.

→ The sequence 8, 11, 9, 1, 4, 6, 12, 10, 5, 7 contain 10 terms.

note $10 = 3^2+1$,

→ There are four increasing subsequences of length four, namely 1, 4, 6, 12;
1, 4, 6, 7;
1, 4, 6, 10;
1, 4, 5, 7

Permutations & Combinations

A permutation of a set of distinct objects is an ordered arrangement of these objects.

An ordered arrangement of r-elements of a set is called an r-permutation.

⑧ Let $S = \{a, b, c\}$ The 2-permutations of 'S' are the ordered arrangements a,b; a,c; b,c; c,b; c,a; b,a;

$P(3,2) = 6$.

$\underbrace{3 \cdot 2}_{\text{Product rule}} = 6$

→ An unordered selection of objects.

② How many diff committees of 3-students can be formed from a group of four students?

$\{a, b, c, d\}$

$\Rightarrow$ chosing four = chosing one & leave it

Binomial Co-efficients

$\binom{n}{r}$ — This no. is called binomial coefficients.

Let x, y be variables, & n be a non-negative int

$$(x+y)^n = \sum_{j=0}^{n} \binom{n}{j} x^{n-j} y^j$$

$$= \binom{n}{0} x^n + \binom{n}{1} x^{n-1} y + \binom{n}{2} x^{n-2} y^2 + \cdots \binom{n}{n-1} x y^{n-1} + \binom{n}{n} y^n$$

(c) what is the expansion of $(x+y)^4$?

$$(x+y)^4 = \sum_{j=0}^{4} \binom{4}{j} x^{4-j} y^j$$

$$= \binom{4}{0}x^4 + \binom{4}{1}x^3y + \binom{4}{2}x^2y^2 + \binom{4}{3}xy^3 + \binom{4}{4}y^4$$

$$= x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + y^4$$

(d) what is the coefficient of $x^{12}y^{13}$ in $(x+y)^{25}$?

$$\binom{25}{13} = \frac{25!}{13!\,12!} = \sum_{j=0}^{25} \binom{25}{j}$$

$$= 5,200,300$$

(e) $x^{12}y^{13}$ in the expansion $(2x-3y)^{25}$?

$$(2x+(-3y))^{25} = \sum_{j=0}^{25} \binom{25}{j} (2x)^{25-j} (-3y)^j$$

$$\binom{25}{13} (2)^{12} (-3)^{13} = \frac{25!}{-13!\,12!} 2^{12} 3^{13}$$

(a) Let n be a non-negative integer. Then

$$\sum_{k=0}^{n} \binom{n}{k} = 2^n$$

Proof: Using Binomial theorem $x=1$ & $y=1$

$$2^n = (1+1)^n = \sum_{k=0}^{n} \binom{n}{k} 1^k 1^{n-k} = \sum_{k=0}^{n} \binom{n}{k}$$

(d) Let n be a positive integer. Then

$$\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0$$

Use Binomial $x=-1$ & $y=1$

$$\therefore 0 = 0^n = ((-1)+1)^n = \sum_{k=0}^{n} \binom{n}{k} (-1)^k 1^{n-k}$$

$$= \sum_{k=0}^{n} \binom{n}{k} (-1)^k$$

→ Let n be a non-negative integer. Then

$$\sum_{k=0}^{n} 2^k \binom{n}{k} = 3^n \qquad x=1,\ y=2$$

$$(1+2)^n = \sum_{k=0}^{n} \binom{n}{k} (1)^{n-k} 2^k$$

$$= \sum_{k=0}^{n} \binom{n}{k} 2^k$$

Pascal's Identity & Triangle

Theorem: Let 'n' & 'k' be the integers $n \geq k$, Then

$$\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$$

$\binom{0}{0}$

$\binom{1}{0}$ $\binom{1}{1}$

$\binom{2}{0}$ $\binom{2}{1}$ $\binom{2}{2}$

$\binom{3}{0}$ $\binom{3}{1}$ $\binom{3}{2}$ $\binom{3}{3}$

$\binom{4}{0}$ $\binom{4}{1}$ $\binom{4}{2}$ $\binom{4}{3}$ $\binom{4}{4}$

$\binom{5}{0}$ $\binom{5}{1}$ $\binom{5}{2}$ $\binom{5}{3}$ $\binom{5}{4}$ $\binom{5}{5}$

$\binom{6}{0}$ $\binom{6}{1}$ $\binom{6}{2}$ $\binom{6}{3}$ $\binom{6}{4}$ $\binom{6}{5}$ $\binom{6}{6}$

$\binom{7}{0}$ $\binom{7}{1}$ $\binom{7}{2}$ $\binom{7}{3}$ $\binom{7}{4}$ $\binom{7}{5}$ $\binom{7}{6}$ $\binom{7}{7}$

$\binom{6}{4} + \binom{6}{5} = \binom{7}{5}$

VANDERMONDE'n IDENTITY

Let m, n & r be non-ve integers with r not exceeding either m or n.

$$\binom{m+n}{r} = \sum_{k=0}^{r} \binom{m}{r-k}\binom{n}{k}$$

26|81

1, 9, 13, 14, 21, 22, 33, 36, 39, 43, 47, 56, 60, 702, 306, 38, -23 - Absent

53 57

29|8 8, 29, 33, 34, 39, 40, 47, 53, ~~56~~, 56, 57, 303, 306, 308, 314

31|8 1, 2, 3, 4, ~~5~~, 9, 10, 11, 13, 15, 17, 18, 19, 20, 22, 24, 26, 29, 33, 35, 36, 37, 38, 39, 41, 43, 44, 48, 50, ~~51~~, 52, 54, 56, ~~57~~, 58, 60, ~~702~~, ~~306~~, 308,

⑤ Find a recurrence relation ~~can be used to Count bit strings of a specified length that~~ & give initial conditions for the no. of bit strings of length 'n' that do not have two consecutive 0's. How many such bit strings are there of length five?

Let a_n = The no. of bit strings of length 'n' that do not have two consecutive 0's.

Apply sum rule.

a_n = The no. of bit strings of length 'n' that do not have two consecutive 0's ~~exist~~ = the no. of such string ending with '1'

+ The no. of such bit strings ending with a '1'.

$\therefore n \geq 3$.

No. of bit strings of length 'n' with no two consecutive 0's

End with a 1 : [Any bit string of length n-1 with no two consecutive 0's] 1 ... a_{n-1}.

End with a 0 : [Any bit strings of length n-2 with no two consecutive 0's] 1 0 ... a_{n-2}

$$a_n = a_{n-1} + a_{n-2}$$

$n \geq 3$

$\therefore a_1 = 2$ bit string of length '1' have 0 & 1

$\therefore a_2 = 3$ " " " 2 - 00, 01, 10, 11

$a_3 = a_2 + a_1$, $a_4 = a_3 + a_2$, $a_5 = a_4 + a_3 = 13$

String of decimal digits ⇒ ----------

How n- digit string obtained from a strings of 'n-1' digits.

1) n + n-1 other than 0's. = $9a_{n-1}$
valid valid.

2) n-1 + 0
not valid

$(10^{n-1} + a_{n-1})$ a_n

$\therefore a_n = 9a_{n-1} + (10^{n-1} - a_{n-1})$

$a_n = 8a_{n-1} + 10^{n-1}$

Recursive definitions and Structural Induction

Recursion: Define the object in terms of itself is called Recursion.

∴ Recursively defined Function:

∴ Basis Step: Specify the value of the function at zero.

∴ Recursive Step: Give a rule for finding its value at an integer from its values at smaller integers.

Such a definition is called a recursive or inductive definition.

Recursively defined functions are well defined. ie, for every

⑥ Suppose that f is defined recursively by for integer, the value of the function at this integer is determined in unambiguous way.

$f(0) = 3$,

$f(n+1) = 2f(n) + 3$

Find $f(1), f(2), f(3)$ and $f(4)$

⑥ $f(1) = 2 \times 3 + 3 = 9$

$f(2) = 2 \times 9 + 3 = 21$

$f(3) = 2 \times 21 + 3 = 45$

$f(4) = 2 \times 45 + 3 = 93.$

⑦ Give an inductive definition of the factorial function

$F(n) = n!$

Basis Step: the initial value of this function, namely

$F(0) = 1$

∴ Recursive Step: $F(n+1) = (n+1) F(n)$

Rule for finding $F(n+1)$ from $F(n)$, this is obtained by noting that $(n+1)!$ is computed from $n!$ by multiplying by $n+1$.

$F(5) = 5 \cdot F(4) = 5 \cdot 4 F(3) = 5 \cdot 4 \cdot 3 F(2)$
$= 5 \cdot 4 \cdot 3 \cdot 2 F(1) = 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 \cdot F(0)$
$= 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1 \cdot 1 = 120$

Proving Results about Sets:-

Mathematical induction can be used to prove many results about sets.

⑥ Use M.Induction to show that if 'S' is a finite set with 'n' elements where 'n' is a non-negative integer, then 'S' has 2^n subsets.

Sol:- Let P(n) be the proposition that a set with 'n' elements has 2^n subsets.

∴ Basis step:- P(0) is true, because a set with zero elements, the empty set, has exactly $2^0 = 1$ subset, namely, itself.

∴ Inductive step:-

We assume that P(k) is true for the non-negative integer 'k', i.e., we assume that every set with 'k' elements has 2^k subsets.

Assume the P(k+1), which is the stmt that every set with k+1 elements has 2^{k+1} subsets, must also be true.

Let 'T' be a set with k+1 elements.

$T = S \cup \{a\}$ where a is one of the element of 'T'

and $S = T - \{a\}$ $(\because |S| = k)$

⇒ For each subset 'X' of 'S' there are exactly two subsets of 'T',

X & $X \cup \{a\}$

T consists of all distinct subset.

$T = 2 \cdot 2^k = 2^{k+1}$ Proved.

Principle of Strong M.I

Let P(n) is true for all the integer 'n', where P(n) is a propositional function. We complete two steps.

Basis step:- We verify the proposition P(1) is true.

Inductive step:- We show that conditional stmt

$[P(1) \wedge P(2) \wedge \dots \wedge P(k)] \rightarrow P(k+1)$

is True ∀ the integers 'k'

⑧ Using Principle-I. Prove that any integer $n \geq 2$ is either a prime or a product of primes.

Sol:- P(n) — n is a prime or product of prime.

→ As '2' is a prime no. P(2) is true.

P(3) is T

P(4) is product of prime.

→ P(n) is True for $2 \leq n \leq k$, $(k \geq 4)$

i.e., P(2), P(3), P(4) — — P(k)

Now for $n = k+1$

① If k+1 is a prime P(k+1) is T.

" " is not a then

$(k+1) = uv$, when $2 \leq u \leq k$ & $2 \leq v \leq k$

(4) Prove that $7^{2n} + 2^{3n-3} \cdot 3^{n-1}$ is divisible by 25 $\forall$ the integers.

Soln Let $P(n) = 7^{2n} + 2^{3n-3} \cdot 3^{n-1}$ is divisible by 25.

For $n=1$

Basis $P(1) \to 7^2 + 2^0 \cdot 3^0 \Rightarrow 49+1 = 50 \mid 25.$

$P(1)$ is true.

Inductive $n = k$ i.e., $7^{2k} + 2^{3k-3} \cdot 3^{k-1}$

$7^{2k} + 2^{3k-3} \cdot 3^{k-1} = 25p, \quad (p \in Z)$

$n = k+1$

$7^{2k+2} + 2^{3k+3-3} \cdot 3^{k+1-1}$

$\Rightarrow 7^{2k+2} + 2^{3k} \cdot 3^{k} + 7^2 \cdot 2^{3k-3} \cdot 3^{k-1} - 7 \cdot 2^{3k-3} \cdot 3^{k-1}$

$\Rightarrow 7^2\left(7^{2k} + 2^{3k-3} \cdot 3^{k-1}\right) - 7 \cdot 2^{3k-3} \cdot 3^{k-1} + 2^{3k} \cdot 3^{k}$

$\Rightarrow 7^2 (25p) - 2^{3k-3} \cdot 3^{k-1} \left(7^2 - 2^3 \cdot 3^1\right)$

$\Rightarrow 7^2 (25p) - 2^{3k-3} \cdot 3^{k-1} \cdot 25$

$= 25\left(7^2 p - 2^{3k-3} \cdot 3^{k-1}\right)$

Binary trees — Extended binary
— full binary

(5) Extended binary

Basis : root σ, An empty set is an extended binary

Recursive : T_1, T_2 are connected to root r by an edge. T_1, T_2 may or may not be the or empty tree.

Basis •

Step ①

Step ②

(6) full binary

Basis : consists of a single vertex r.

Recursive : If T_1 and T_2 are full binary trees, there is a full binary tree, denoted by T_1, T_2. consisting of a root r together with edges connecting the root to each of the roots of left subtree T_1 & the right subtree T_2.

Basis •

Step ①

Step ②

Structural Induction

→ Instead of directly applying

Step ①: Results holds for all the elements specified in the basis step.

Step ②: Recursive step: If the result is true for each of the elements used to construct new elements in the recursive step of the definition

Ex: Basis step: Result is true for $p(0)$, if p whenever p is a propositional variable

Recursive step:

p shift is true for

Unit - II

Mathematical Reasoning, Induction & Recursion, Proof Strategy. Sequences and Summation, Mathematical Induction, Recursive definitions and Structural Induction, Recursive algorithms. Counting: Basics of Counting, Pigeonhole Principle, Permutations and Combinations - Binomial Coefficients, Generalized Permutations and Combinations, Generating Permutations & Combinations.

Sequences & Summations

Def: A sequence is a set A is a function f from the subset of the integers (usually $\{0,1,2,\ldots\}$ or $\{1,2,\ldots\}$) to A. The value of a sequence are also called its terms or entries

The value $f(n)$ is usually denoted a_n.

A sequence is often written as $a_0, a_1, a_2, \ldots$

Ex: ① Two sequences

$a_n = \frac{1}{n}$, $1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \ldots$

$b_n = (-1)^n$, $1, -1, 1, -1, \ldots$

② Five ubiquitous sequences.

n^2 0, 1, 4, 9, 16, ...

n^3 0, 1, 8, 27, 64, ...

2^n 0, 2, 4, 8, 16, ...

$n!$ 1, 2, 6, 24, 120, ...

Strings

Def: A set of characters is called an alphabet

Ex: $\{0,1\}$ - the binary alphabet.
$\{0,1,\ldots,9\}$ the decimal alphabet.

Def: A string is a sequence in an alphabet.

Ex: If $f(0) = M$, $f(1) = A$, $f(2) = T$, and $f(3) = H$ then write "MATH".

Problem: Given some initial terms $a_0, a_1, \ldots a_k$ of a sequence, try to construct a rule that is consistent with those initial terms.

Approaches: There are two standard kinds of rule for calculating a generic term a_n.

Def: A recursion for a_n is a function whose arguments are earlier terms in the same sequence.

Def: A closed form for a_n is a formula whose argument is the subscript n.

Ex: ① 1, 3, 5, 7, 9, 11 ——

recursion: $a_0 = 1$ $\quad a_n = a_{n-1} + 2$ for $n \geq 1$

Closed form: $a_n = 2n+1$

$n=0 \quad n=1 \quad n=2$
$a_0=1 \quad a_1=3 \quad a_2=5$

$3 = 1+2$

② 1, 3, 7, 13, 21, 31, 43 ——

recursion: $b_0 = 1$ $\quad b_n = b_{n-1} + 2n$ for $n \geq 1$

Closed form: $b_n = n^2 + n + 1$

③ 1, 1, 2, 3, 5, 8, 13, 21, 34 ——

recursion: $c_0 = 1, \; c_1 = 1$ $\quad c_n = c_{n-1} + c_{n-2}$

Closed form: $c_n = \frac{1}{\sqrt{5}} \left[\alpha^{n+1} - \beta^{n+1} \right]$

Methods of Proof

→ A theorem is a strict, fact or result that can be shown to be true.

→ A proposition can be considered as a less important theorem.

Lemma ——
Corollary ——

Trivial Proof:

$P \to Q$ is T whenever conclusion 'Q' is true, regardless of the truth values of 'P'.

Showing only 'Q' is true to prove $P \to Q$ is known as trivial proof of the stmt $P \to Q$.

④ If 'a' is an integer, then prove that $a^{2n} \geq 1$ for $n \geq 0$.

As $a^0 = 1$ (regardless of value of a) $a^{2n} \geq 1$ for $n \geq 0$

∴ Proved.

Vacuous Proof:

We know $P \to Q$ is 'T' whenever 'P' is false.

$P \to Q$ can easily proved by proving 'P' is false

⑤ If $n > 2$ then $n^2 > 2n$. Prove that $P(0)$ is 'T'.

For $n = 0$, the condition $n > 2$ is False.

∴ $P(n)$ is 'T' for $n = 0$.

Direct Proof :

we start the assumption that 'P' is true, & then use the RoI & already proved theorem & definition to show that 'Q' is also true.

(∵ $P \to Q$ is T whenever 'P' is 'F')

∴ start with assumption 'p' is True)

② S.T. the Squares of an even no. is an even no.

- if n is an even no, then n^2 is also even".

P : n is an even

Q : n^2 " "

$n = 2k$ where $k \in Z$

$n^2 = (2k)^2 = 4k^2 = 2(2k^2)$

$\Rightarrow n^2$ is an even no.

③ S.T Sum of 2 odd nos is an even no.

→ P : a is odd & b is odd

→ Q : a+b is even

$a = 2l+1$, $b = 2m+1$

$a+b = 2l+1+2m+1$

$= 2(l+m+1)$

a+b is even

④ **Proof by Contradiction**

→ It is based on the fact that a statement is either T or F but not both at the same time.

⇒ To prove that a statement 'p' is true, we assume that ~p is true & taking ~p as premise, we drawn a Contradiction 'F' as the Conclusion

~p must = F ∴ $(p \to T)$

① Assume that 'p' is false ⇒ ~p = T

② Show a Contradiction

⑤ ~~S.T $\sqrt{2}$ is an irrational no.~~

⑤ P.S "if 3n+1 is even, then n is odd" use P.B.C

P : 3n+1 is even Q : n is odd

Assume P is T & Q is F.

Let n is even ∴ 3n+1 is even.

Let $n = 2k$ for some k, then

$3n+1 = 3(2k)+1 = 6k+1$

$\because 6k = 2(3k)$

⇒ 6k is even

⇒ 6k+1 is odd

⇒ 3n+1 " "

∴ This is Contradiction 3n+1 is even.

∴ n is not even, n is odd.

Hence

Proof by Contraposition

we use the fact that $p \to q \equiv \neg q \to \neg p$.

(a) P.T. if n^2 is odd, then n is odd.

hyp: p — concl: q

$p \to q \equiv T$

$\neg q \to \neg p$ → if n is even then n^2 is even.

Proof by cases

Some time prove conditional stat as

$(p_1 \vee p_2 \vee \cdots \vee p_n) \to q$

we can easily

$(p_1 \vee p_2 \vee \cdots p_n) \to q$.

$\equiv (p_1 \to q) \wedge (p_2 \to q) \wedge \cdots (p_n \to q)$

(b) Prove that $(n+1)^2 \geq 3^n$ if n is a +ve integer with $n \leq 4$

We need to verify inequality $(n+1)^3 \geq 3^n$

$n = 1, 2, 3, 4$

$n=1$, $(n+1)^3 = 2^3 = 8 \geq 3$

$n=2$ $(n+1)^3 = 3^2 \geq 3^2 \Rightarrow 27 \geq 9$

$n=3$ $(3+1)^3 = 4^2 \Rightarrow 64 \geq 27$

$n=4$ $(4+1)^3 = 5^2 \geq 81\ 125 \geq 81$

$n=5$ $(5+1)^3$, 3^5

$216 \geq 243$

Examples of Proofs by Mathematical Induction

1) Proving summation formulae
2) " Inequalities
3) " Divisibility Results.
4) " Results about sets.
5) " " " Algorithms.

2) Proving Inequalities

(a) Use M.I to prove inequality $n < 2^n$ for all the integers n.

Sol: Let $P(n)$ is the proposition that $n < 2^n$

B. Step: $P(1)$ is true $1 < 2^1 = 2$

In. Step: Assum $P(k)$ is true for all k.

$P(k) \Rightarrow k < 2^k$ $\quad P(k)$ is $T \to P(k+1)$ is T

If $k < 2^k$ then $k+1 < 2^{k+1}$ / $k+1 < 2^{k+1}$ $\Rightarrow$ $k+1$

i.e. $k < k+1 < 2^k$

$k < 2^k$ — (1)

Add '1' on both sides of (1) $1+k < 2^k + 1$

$1+k < 2^k + 2^k$ $\quad (1 \leq 2^k)$ from basis step

$1+k < 2 \cdot 2^k$

$(k+1) < 2^{(k+1)}$

Proved.

(b) $2^n < n!$ for every integer $n \geq 4$.

1. Step: $n \geq 4$

$P(4) \Rightarrow 2^4 = 16 < 24 = 4!$

2. Step: Assume $P(K)$ is True for K with $K \geq 4$ for the +ve integers

$2^K < K!$

$2^{K+1} = 2 \cdot 2^K$ (by def of exponent)

$< 2 \cdot K!$ (by the induction hypothesis)

$< (K+1) \cdot K!$ (bcoz $2 < K+1$)

$= (K+1)!$ (by definition of factorial function)

$2^{K+1} < (K+1)!$

$\therefore$ $P(K+1)$ is true

Inclusion-Exclusion principle

When two tasks can be done at same time, we can't use the sum rule to count the no. of ways to do one of the two tasks

To correctly count the no. of ways to do one of the two tasks, we add the no. of ways to do each of the 2 tasks and then subtract the no. of ways to do both tasks. This technique is called the principle of inclusion-Exclusion

If A_1, A_2 are sets, let T_1 be the task of doing an element from A_1 & T_2 from A_2

Then T_1 in $|A_1|$

T_2 in $|A_2|$

$\therefore$ The no. of ways of doing either T_1 or T_2 is taken as

$$|A_1 \cup A_2| = |A_1| + |A_2| - |A_1 \cap A_2|$$

(a) How many bit strings of length eight either start with a 1bit or end with a 2 bits 00?

Sol:

$A_1 \Rightarrow$ start with 1 $\Rightarrow 2^7$ ways. $= 1 \underbrace{\_\_\_\_\_}_{2^7}$

$A_2 \Rightarrow$ ends with 00 $\Rightarrow 2^6$ ways. $\underbrace{\_\_\_\_\_}_{2^6} 00$

$|A_1 \cap A_2| \Rightarrow$ start with 1 and ends with 00 $\Rightarrow 2^5$ $1 \underbrace{\_\_\_\_\_}_{2^5} 00$

$\therefore |A_1 \cup A_2| = 2^7 + 2^6 - 2^5 \Rightarrow$

$= 128 + 64 - 32$

$= 160$

→ we can extend to more than 2 tasks.

If $T_1, T_2, \ldots T_n$ can be done in $n_1, n_2, \ldots n_n$ ways respectively, and no two of these tasks can be done at the same time.

Then the no. of ways to do these tasks is $n_1 + n_2 + \ldots + n_m$.

Ex: A student can choose a computer project from one of three lists. The three lists contain 23, 15, and 19 possible projects, respectively. How many possible projects are there to choose from?

Soln: The student can choose a project from the first list in 23 ways, from the second list in 15 ways, and from the third list in 19 ways.

$\therefore$ $23+15+19 \Rightarrow$ 57 projects to choose.

The sum rule can be phrased in terms of sets as:

If $A_1, A_2, \ldots A_m$ are disjoint sets, Then the no. of elements in the union of these sets is the sum of the no. of elements in them.

Let T_i be the task of choosing an element from A_i for $i = 1, 2, \ldots m$. There are $|A_i|$ ways to do T_i.

$|A_1 \cup A_2 \cup \ldots A_m| = |A_1| + |A_2| + \ldots + |A_m|$

∴ Binomial Co-efficients :-

The no. of r-combinations from a set with n-elements is often denoted by $\binom{n}{r}$. This no is also called a Binomial Co-efficient. Because these no. occur as co-efficients in the expansion of powers of binomial expressions such as $(a+b)^n$.

→ Binomial Theorem gives the power of a binomial expression as sum of terms involving binomial co-efficients.

A binomial expression is simply the sum of two terms, such as $x+y$.

∴ Binomial Theorem :-

Let x, y be variables and 'n' is a non-negative integer. Then

$$(x+y)^n = \sum_{j=0}^{n} \binom{n}{j} x^{n-j} y^j$$

$$(x+y)^n = \binom{n}{0} x^n + \binom{n}{1} x^{n-1} y + \binom{n}{2} x^{n-2} y^2 + \cdots + \binom{n}{n-1} x y^{n-1} + \binom{n}{n} y^n.$$

Q. What is the expansion of $(x+y)^4$?

Soln:

$$(x+y)^4 = \sum_{j=0}^{4} \binom{4}{j} x^{4-j} y^j$$

$$= \binom{4}{0} x^4 + \binom{4}{1} x^3 y + \binom{4}{2} x^2 y^2 + \binom{4}{3} x y^3 + \binom{4}{4} y^4$$

$$\therefore x^4 + 4x^3y + \frac{4!}{2!2!} x^2y^2 + \frac{4!}{3!} xy^3 + y^4$$

$\therefore (x+y)^4 = x^4 + 4x^3y + 6x^2y^2 + 4xy^3 + y^4$.

(b) what is the coefficient of $x^{12}y^{13}$ in the expansion of $(x+y)^{25}$?

Sol'n From the Binomial Theorem it follows that the coefficient is

$$\binom{25}{13} = \frac{25!}{12!\,13!} = \frac{14\times15\times16\times17\times18\times19\times20\times21\times22\times23\times24\times25}{1\times2\times3\times4\times5\times6\times7\times8\times9\times10\times11\times12\times13}$$

$$= 17\times19\times7\times4\times23\times25$$

$$= 17\times19\times23\times25\times28$$

$$= 5,200,300$$

(c) what is the coefficient of $x^{12}y^{13}$ in the expansion of $(2x-3y)^{25}$?

Sol'n By Binomial Theorem $(2x+(-3y))^{25}$

$$x^{12}y^{13} \Rightarrow \binom{25}{13} = -\frac{25!}{12!\,13!}\,2^{12}\,3^{13}$$

$$= \frac{n!}{(k-1)!\,(n-k+1)!} + \frac{n!}{k!\,(n-k)!}$$

$$= \frac{k\,n! + n!\,(n-k+1)}{k!\,(n-k+1)!}$$

$$= \frac{kn! + n!\,(n+1) - kn!}{k!\,(n-k+1)!}$$

$$= \frac{n!\,(n+1)}{k!\,(n-k+1)!}$$

$$= \frac{(n+1)!}{k!\,(n-k+1)!}$$

$$= \binom{n+1}{k}$$

→ It is useful in the computation of binomial co-efficients since only addition of integers is needed.

→ It is the basis for a geometric arrangement of the binomial co-efficients in a triangle as below

(21)

(15)

① $\sum_{k=0}^{n} \binom{n}{k} = 2^n$

② $\sum_{k=0}^{n} (-1)^k \binom{n}{k} = 0$

③ $\sum_{k=0}^{n} 2^k \binom{n}{k} = 3^n$

PASCAL'S IDENTITY :-

Let 'n' and 'k' be positive integers with $n \geq k$

then $\binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$

proof :- Suppose that 'T' is a set containing $n+1$ elements

Let 'a' be an element in T, and let $S = T - \{a\}$

Note that there are $\binom{n+1}{k}$ subsets of T containing 'k' elements. However, a subset of T with 'k' elements either contains a together with $k-1$ elements of 'S', or contains k elements of 'S' and does not contain 'a'. Since there are $\binom{n}{k-1}$ subsets of $k-1$ elements of 'S' there are $\binom{n}{k-1}$ subsets of 'k' elements of 'T' that contain 'a'. And there are $\binom{n}{k}$ subsets of k elements of 'T' that do not contain 'a'.

$\therefore \binom{n+1}{k} = \binom{n}{k-1} + \binom{n}{k}$

Generalized Pigeonhole Principle

If N objects are placed into 'k' boxes, then there is atleast one box containing atleast $\lceil N/k \rceil$ objects.

② Among 100 people there is atleast $\lceil 100/12 \rceil = 9$, who were born in the same month.

③ During the month with 30 days, a base ball team plays atleast one game a day, but no more than 45 games. Show that there must be a period of some no. of consecutive days during which the team must play exactly 14 games.

Sol :- Let a_j - be the no. of games played on or before the j^{th} day of the month.

$\therefore$ $a_1, a_2 \ldots a_{30}$ is an increasing sequence of distinct $+ve$ integers., with $\boxed{1 \leq a_j \leq 45}$

Moreover $a_1+14, a_2+14 \ldots a_{30}+14$

$15 \leq a_j + 14 \leq 59.$

The 60 $+ve$ integers $a_1, a_2 \ldots a_{30}, a_1+14, a_2+14 \ldots a_{30}+14$ are all $\boxed{\leq 59}$

There must be indices $i \neq j$ with $a_i = a_j + 14$,

This means exactly 14 games were played from day $j+1$ to day i.

15 – W
10 – S
) cable.

→ A cable can be used to directly connect a W to Server.

→ For each server, only one direct connection to that server can be active at any time.

Connect W_k to S_k $k = 1, 2, \ldots, 10$.

& each $W_{11}, W_{12}, W_{13}, W_{14} \& W_{15}$ to all 10 servers.

Total $10 + 50 \Rightarrow 60$ direct Connection

Clearly any set of 10 or fewer workstations can simultaneously access diff. servers.

Unit-II

9/12 (2 hrs)

Methods of Proof :

→ A theorem is a statement that can be shown to be true (Theorems are sometimes called propositions, facts, or results)

→ Proof : A theorem is true with a sequence of steps that form an argument is called a proof

→ The steps used in a proof can include ~~the~~ axioms or postulates, which are underlying ~~assumptions~~ about mathematical structure.

The rules of inference : which are the means used to draw conclusions from other assertions, tie together the steps of proof.

	Rule of Inference	Tautology	name
①	$\frac{p}{\therefore p \vee q}$	$p \to (p \vee q)$	law of addition
②	$\frac{p \wedge q}{\therefore p}$	$p \wedge q \to p$	Simplification
③	$\frac{p \quad q}{\therefore p \wedge q}$	$((p) \wedge (q)) \to p \wedge q$	Conjunction

④ $\dfrac{\begin{array}{l}p\\ p\to q\end{array}}{\therefore q}$ $\quad [p\wedge(p\to q)]\to q$ Modus ponens

⑤ $\dfrac{\begin{array}{l}\neg q\\ p\to q\end{array}}{\therefore \neg p}$ $\quad [\neg q\wedge(p\to q)]$ Modus tollens

⑥ $\dfrac{\begin{array}{l}p\to q\\ q\to r\end{array}}{\therefore p\to r}$ $\quad [(p\to q)\wedge(q\to r)]\to(p\to r)$ Hypothetical Syllogism

⑦ $\dfrac{\begin{array}{l}p\vee q\\ \neg p\end{array}}{\therefore q}$ $\quad [(p\vee q)\wedge\neg p]\to q$ Disjunctive Syllogism

⑧ $\dfrac{\begin{array}{l}p\vee q\\ \neg p\vee r\end{array}}{\therefore q\vee r}$ $\quad [(p\vee q)\wedge(\neg p\vee r)]\to(q\vee r)$ Resolution.

Stmt: The rule of inference (transformation rule) is a function from sets of formula to formula. The argument is called the premise set. (or simply premises) & the value the conclusion

→ A rule of inference need not preserve any semantic property such as truth or validity. ⑦ ⑧

→ May preserve eg: the property of being the conjunction of the subformula of the longest formula in the premise set.

Generally

premise #1
premise #2
⋮
Conclusion.

Def: valid argument:

when argument is said to be valid if whenever all the hypothesis are true the conclusion are also true.

Def: Fallacy:

Incorrect reasoning is called fallacy. They are not tautologies.

we have 2 kinds of fallacies

① The fallacy of affirming the conclusion:

The proposition $[(p\to q)\wedge q]\to p$ is not a tautology it is false when 'p' is false and q is true.

② The fallacy of denying the hypothesis.

The proposition $[(p\to q)\wedge\neg p)]\to\neg q$ this proposition is not a tautology. it is false when p is false and q is true.

Rules of inference for quantified propositions:-

Rule of Inference	Name
$\frac{\forall x\, P(x)}{\therefore P(c)}$	Universal instantiation
$\frac{P(c) \text{ for an arbitary } c}{\therefore \forall x\, P(x)}$	Universal generalization
$\frac{\exists x\, P(x)}{\therefore P(c) \text{ for some element } c}$	Existential instantiation
$\frac{P(c) \text{ for some element } c}{\therefore \exists x\, P(x)}$	Existential generalization

(a) which rule of inference is used in the following arguments:

If it is rain then the pool will be closed
It is raining therefore the pool is closed

$$\frac{p \rightarrow q \quad p}{\therefore q}$$

Modus ponens.

(b) If it snows today the university will be closed
The university is not closed (3)
$\therefore$ It didn't snow today (1)

$$\frac{p \rightarrow q \quad \neg q}{\therefore \neg p} \qquad \frac{\neg q \quad p \rightarrow q}{\therefore \neg p}$$

$\Rightarrow$ Modus Tollens

(c) If I go & work all night on this homework, then I can answer all the exercises.
If I answer all the exercises I will understand the material.
$\therefore$ If I work all night on this homework, then I will understand the material.

$$\frac{p \rightarrow q \quad q \rightarrow r}{\therefore p \rightarrow r}$$

Hypothetical Syllogism.

(d) Construct an argument using rules of inference to show that the hypotheses, "Randy work hard", "If Randy works hard, then he is a dull boy" and "If Randy is a dull boy then he will not get the job" imply the conclusion.

"Randy will not get the job"

p : Randy works hard
q : he is a dull boy
r : he will not get a job

$$\frac{p \quad p \to q \quad q \to r}{\therefore r}$$

$$\frac{p \quad p \to q \quad q \to r}{\therefore r}$$

④ Construct an argument using rules of inference to show that the hypothesis "If it does not rain or if it is not foggy, then the sailing race will be held and the lifesaving demonstration will go on", "If the sailing race is held, then the trophy will be awarded", and "The trophy was not awarded" imply the conclusion "It rained"

Sol:

p : It does not rain
q : It is not foggy
r : Sailing race held
s : lifesaving demonstration held
t : trophy is awarded

$$\frac{(p \vee q) \to (r \wedge s) \quad \neg r \to t \quad \neg t}{\therefore \neg p}$$

④ ④

$$\frac{r \wedge s}{\therefore r} \quad \text{Simplification}$$

$$\frac{(p \vee q) \to r \quad r \to t}{(p \vee q) \to t} \quad \text{Hypothetical Syllogism}$$

$$\frac{\neg t \quad (p \vee q) \to t}{\neg (p \vee q)} \quad \text{Modus tollens}$$

$\neg p \wedge \neg q$ → demorgan's law

$$\frac{\neg p \wedge \neg q}{\therefore \neg q} \quad \text{not raining}$$

Methods of proof of Implications:

→ All theorems are basically implications we know that $p \to q$ is true always except when p is true and q is false based on this we have diff ways of proving an implication

① Direct Proof: In this proof we assume that 'p' is true and we rules of inference and other known results to show that 'q' is also true.

Ex: Give a direct proof of if 'n' is odd then n^2 is odd.

p : n is odd
q : n^2 is odd

let n be odd

$\Rightarrow n = 2n+1$ $\quad k \in$ integers
$n^2 = (2k+1)^2$
$n^2 = 4k^2+4k+1$
$= 4k(k+1)+1$
= which is odd
$\therefore$ n^2 is odd.

② Indirect Proof: we know the contrapositive of $p \to q$ is $\neg q \to \neg p$ and they are equivalent
$\therefore$ $p \to q$ is proving by $\neg q \to \neg p$ such a proof is called indirect proof.

→ Give an indirect proof of the following stmt.

If $3n+2$ is odd then 'n' is odd

→ we will assume 'n' is not odd

i.e, 'n' is even

$n = 2k$

Consider $3n+2 = 3(2k)+2$

$= 2[3k+1]$

$=$ even

$= \neg p$

p : $3n+2$ is odd

q : n is odd

③ Vacuous proof :-

In $p \to q$, let p be false then from defination of implication $p \to q$ is true.

because the stmt has the forms $F \to F$, $F \to T$, and hence is true.

Consequently, if it can be shown that 'p' is false, the the proof is known as vacuous proof.

Ex: Show that the proposition $P(0)$ is true where $P(n)$ is the propositional function "If $n>1$, then $n^2>n$".

Soln: $P(0)$ is the implication "If $0>1$, then $0^2>0$"

④ Trivial Proof :-

Let the conclusion 'q' of an implications $p \to q$ is true.

Then $p \to q$ is true.

Since the stmt has the form $T \to T$ or $F \to T$, which are true.

∴ It can be shown that 'q' is true, irrespective of 'p'. then a proof is called a trivial Proof

Ex: Let $P(n)$ be "If a and b are the integers with $a \geq b$, then $a^n \geq b^n$" Show that the proposition $P(0)$ is true.

Soln: The proposition $P(0)$ is

"If $a \geq b$, then $a^0 \geq b^0$"

whatever be the value of a & b $P(0)$ is true

⑤ Proofs by contradiction :-

Suppose that the contradiction 'q' can be found so that $\neg p \to q$ is true.

then the proposition $\neg p$ must be false.

∴ p must be true.

Ex: proof by contradiction if $3n+2$ is odd then 'n' is odd.

→ Assume $3n+2$ is odd then 'n' is not odd

n is even, $n = 2k$

∴ $3n+2 \Rightarrow 7(2k)+2 \Rightarrow$ even

This is a contradiction because $3n+2$ is odd.

∴ [illegible]

⑥ Proof by cases:

It is used, To prove an implication of the form

$$(P_1 \vee P_2 \vee \cdots \vee P_n) \rightarrow q$$

~~it or prove that~~
~~the tautology~~

$$[(P_1 \vee P_2 \vee \cdots \vee P_n)] \leftrightarrow [(P_1 \rightarrow q) \wedge (P_2 \rightarrow q) \wedge \cdots \wedge (P_n \rightarrow q)]$$

can be used as a rule of inference.

To prove that take $P_1 \rightarrow q, P_2 \rightarrow q \cdots P_n \rightarrow q$ separately and take their conjunctions.

$$(P_1 \vee P_2 \vee \cdots \vee P_n) \rightarrow q$$

$$\equiv$$

$$(P_1 \rightarrow q) \wedge (P_2 \rightarrow q) \wedge \cdots \wedge (P_n \rightarrow q)$$

i.e. $P_i \rightarrow q$, $i = 1, 2, \ldots n$ is called proof by cases.

Ex: Prove the implication using proof by cases.

~ If n is an integer not divisible by 3, then $n^2 \equiv 1 \pmod 3$.

p : n is not divisible by 3

q : $n^2 \equiv 1 \pmod 3$

→ If n is not divisible by 3 then $n \equiv 1 \pmod 3$, or $n \equiv 2 \pmod 3$ (various possible cases)

Let P_1 : $n \equiv 1 \pmod 3$

P_2 : $n \equiv 2 \pmod 3$

⑦ Proof of Equivalence: ⑦

To prove a theorem i.e, a biconditional, i.e, $p \leftrightarrow q$ where p & q are propositions

$$p \leftrightarrow q \equiv ((p \rightarrow q) \wedge (q \rightarrow p))$$

we shall prove $P_1 \vee P_2 \to q$ by the cases

$\therefore$ prove: $(P_1 \to q) \wedge (P_2 \to q)$

for $P_1 \to q$

$n \equiv 1 \bmod 3 \Rightarrow 3 \mid n-1$

$\Rightarrow (n-1) = 3k$ for any k

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

$n^2 = 9k^2 + 6k + 1$

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

$n^2 - 1 = 3k(3k+2)$

$\Rightarrow 3 \mid n^2 - 1$

$n^2 \equiv 1 \bmod 3$

$P_2 \to q$

$n \equiv 2 \bmod 3 \Rightarrow 3 \mid n-2$

$n - 2 = 3k$ for any k

$n^2 = (3k+2)^2$

$n^2 = 9k^2 + 12k + 4$

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

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

$\Rightarrow 3 \mid n^2 - 1$

$n^2 \equiv 1 \bmod 3$

Sequences :

(8) (4)

→ Sequence is used to represent ordered list of elements.

→ used to represent solutions to certain counting problems.

Def :① A sequence is a function from a subset of the set of integers (usually either the set $\{0, 1, 2, \ldots\}$ or the set $\{1, 2, 3, \ldots\}$) to a set 'S'.

we use the notation a_n to denote the image of the integer 'n', i.e a_n is a term of sequence

Ex : Consider the sequence $\{a_n\}$, where $a_n = 1/n$

$\therefore a_1, a_2, \ldots a_n \Rightarrow \{1, 1/2, 1/3, \ldots 1/n\}$

Def② A geometric progression is a sequence of the form $a, ar, ar^2, \ldots ar^n$

where the initial term a, & common ratio r are real nos.

Ex → $\{b_n\}$ with $b_n = (-1)^n$

→ $\{c_n\}$ with $c_n = 2.5^n$

Def③ An arithmetic progression is a sequence of the form. $a, a+d, a+2d, \ldots a+nd$.

initial term a, common difference d

Ex → $\{s_n\}$ with $s_n = -1 + 4n$, $-1, 3, 7, 11 \ldots$

$\{t_n\}$ with $t_n = 7 - 3n$ $7, 4, 1, -2, \ldots$

→ formula from the sequence

Ex-① The first 10 terms are 5, 11, 17, 23, 29, 35, 41, 47, 53, 59 the expression?

→ $5+6(n-1) \Rightarrow$ 5, 11, 17, 23 ——

$n \to 0, 1, 2, \ldots n$

② 1, 7, 25, 79, 241, 727, 2185, 6559, 19681, 59047

$a_n = 3^n - 2$

③ 3, 6, 12, 24, 48,

$a_n = 3.2^n$

④ 2, 16, 54, 128, 250, 432, 686

$a_n = 2, n^3$

Summations

The notation used to express the sum of the terms $a_m, a_{m+1}, \ldots a_n$ from the sequence $\{a_n\}$

i.e. $\boxed{\sum_{j=m}^{n} a_j \quad \text{or} \quad \sum_{j=m}^{n} a_j}$

→ lower limit is m & upper limit n.

Ex: what is the value of $\sum_{j=1}^{5} j^2$?

$= 1+4+9+16+25$

$\sum_{j=1}^{5} j^2 = 55$

Ex: Compute double sums?

① $\sum_{i=1}^{3} \sum_{j=1}^{2} (i-j)$

$\Rightarrow \sum_{i=1}^{3} ((i-1)+(i-2))$

$\Rightarrow \sum_{i=1}^{3} (2i-3)$

$\Rightarrow -2+1+3$

$\Rightarrow 2$

② $\sum_{i=0}^{2} \sum_{j=0}^{3} i^2 j^3$

Sol: $\Rightarrow \sum_{i=0}^{2} (0+i^2+8i^2+27i^2)$

$= \sum_{i=0}^{2} (36 i^2)$

$= 0+36+144$

$= 180$

Some Useful Summation Formulae

Sum	Closed-form
$\sum_{k=0}^{n} ar^k (r \neq 0)$	$\frac{ar^{n+1} - a}{r-1}$, $r \neq 1$
$\sum_{k=1}^{n} k$	$\frac{n(n+1)}{2}$
$\sum_{k=1}^{n} k^2$	$\frac{n(n+1)(2n+1)}{6}$
$\sum_{k=1}^{n} k^3$	$\frac{n^2(n+1)^2}{4}$
$\sum_{k=0}^{\infty} x^k, \lvert x \rvert < 1$	$\frac{1}{1-x}$
$\sum_{k=1}^{\infty} kx^{k-1}, \lvert x \rvert < 1$	$\frac{1}{(1-x)^2}$

$k=j+1$
$j=0$
$k=1$

Cardinality :-

→ The sets A & B have the same cardinality iff there is a one-to-one correspondence from A to B.

→ A set is either finite or has the same cardinality as the set of the integers is called countable. A set that is not countable is called uncountable

(2) Determine whether each of these sets is countable or uncountable. For those that are countable, (10) exhibit a one-to-one correspondence b/w the set of natural nos. is and that set (c)

(a) The negative integers.

$f(n) = -n$

1 2 3 4 5
↕ ↕ ↕ ↕ ↕
-1 -2 -3 -4 -5

Countable

(b) The even integers.

$f(n) = 2n$

1 2 3 4 5
↕ ↕ ↕ ↕ ↕
2 4 6 8 10

Countable 0, 2, -2, 4, -4

(c) The real nos. b/w 0 and 1

Uncountable

(d) int that is multiple of 7

$f(n) = 7n$

1 2 3 4
7 14 21 28

Countable

0, 7, -7, 14, -14 —

Mathematical Induction:

→ It is a method of mathematical proof typically used to establish that a given stmt is true of all natural nos. It is proving that the first stmt in the infinite sequence of stmts is true, and then proving that if any one stmt in the infinite sequence of stmt is true, then so is the next one

Proof consists of 2 steps:-

① The basis (Basic case) :- showing that the stmt holds when $n=0$ show the positin $P(n)$ is true

② The inductive step :- Showing that if the stmt holds for some 'n', then the stmt also holds when $n+1$ is substituted for n. we show implication $P(n) \rightarrow P(n+1)$ $\forall n$ is true

Ex:- Use the mathematical induction to prove that the sum of the first 'n' odd +ve integers is n^2.

Basis Step :- $P(1)$ states that sum of the first odd +ve integer is 1^2

$P(1) \Rightarrow$ True $\Rightarrow$ Sum of first odd +ve int $= 1$

Inductive step :- To complete the inductive step we must show that $P(k) \rightarrow P(k+1)$

$P(k)$ is true for integer k.

i.e. $1+3+5+ - - +(2k-1) = k^2$

$P(k+1)$ is true assume that $P(k)$ is true (i) (ii)

$1+3+5+ - - +(2k-1)+(2k+1) = (k+1)^2$

$1+3+5+ - - +(2k-1)+(2k+1) = k^2+2k+1$

$= (k+1)^2$

$\therefore \forall n P(n)$ is true using mathematical induction

(a) Use the mathematical induction to prove that $2^n < n!$ for every +ve integer n with $n \geq 4$

Stt

Basis Step :- $n \geq 4$ required $P(4) \Rightarrow 2^4 = 16 < 4! = 24$

Inductive step :- Assume $P(k)$ is true i.e $2^k < k!$

s.T. $P(k+1)$ is true

$2^{k+1} < (k+1)!$

$2^k < k!$

$2^{k+1} = 2.2^k$ (by def of expont) $2.2^k < k! \times 2$

$< 2.k!$ (by inductive hypothesis) $2^{k+1} < (k+1)k!$

$< (k+1)k!$ (because $2 < (k+1)$) $2^{k+1} < (k+1)!$

$2k!$

$k \Rightarrow 3$

$k! \ 2 \times 6 \Rightarrow 12$

$2.k! \ 24$

$k \Rightarrow 4$

$k! \Rightarrow 24$

$2k! \Rightarrow 120$

$6! \Rightarrow 12.$

$(k+1)! \Rightarrow$

$k!$

$5 \longrightarrow k! \Rightarrow 120$

$5 \quad 2k! \Rightarrow 240$

+80

Strong Induction:

Basis step :- The proposition P(1) is shown to be true.

Inductive step :- It is shown that [P(1) ∧ P(2) ∧ ... P(k)] → P(k+1) is true for every the integer k.

Ex:- Prove that every amount of 12 cents or more can be formed by using just 4-cents & 5-cents.

M. Induction:

B. Step :- Postage of 12 cents formed by 3-cents

I. Step :- P(k) is true, so that postage of k cents can be formed using 4-cents & 5cent stamps

① → Atleast 4 cents.

∴ for k+1 5 cents.

k ≥ 12 → At least 5cents

② → 3 – 5 cents

k+1 3 – 4 cents.

S. Induction :- B. step :- 12, 13, 14, 15 using. 4c, 2*4c, 1-5c, (3-4c, 1-5c) 3-5c.

I. step :- Let k ≥ 15 Assume that j cents, where 12 ≤ j < k. To for postage k+1 cents use the stamps from k-3.

P(k+1) is true assume that P(k) is true ① ②

$1+3+5+\dots+(2k-1)+(2k+1) = (k+1)^2$

$1+3+5+\dots+(2k-1)+(2k+1) = k^2+2k+1$

$= (k+1)^2$

∴ ∀n P(n) is true using mathematical induction

② Use the mathematical induction to prove that $2^n < n!$ for every the integer n with $n \geq 4$

Sol Basis Step's $n \geq 4$ required P(4) ⇒ $2^4 = 16 < 4! = 24$

Inductive step :- Assum P(k) is true i.e. $2^k < k!$

S.T. P(k+1) is true

$2^{k+1} < (k+1)!$

$2^k < k!$

$2^{k+1} = 2.2^k$ (by def of expo) $2.2^k < k!$ ∵ 2

$< 2.k!$ (by induction hypothesis) $2^{k+1} < (k+1)k!$

$< (k+1)k!$ (because $2 < k+1$) $2^{k+1} < (k+1)!$

2k!

k ⇒ 7

k! 2×5 ⇒ 12

2k! 24

k ⇒ 4

k! ⇒ 24

2k! ⇒ 120

$k! \geq 12$.

$(k+1)! \geq k!$

5 → k! ⇒ 120

5 2k! ⇒ 240

+80

(12)

(ii) $P(n): n^3 - n$ is divisible by 3.

Basic step :- to show

$P(1)$ is true

$P(1) = 0$ is divisible by 3

Inductive step :-

Assume $P(n)$ to be true $\Rightarrow n^3 - n = 3k$

$\therefore P(n+1) = (n+1)^3 - (n+1)$

$= n^3 + 1 + 3n(n+1) - (n+1)$

$= n^3 + 1 + (3n-1)(n+1)$

$= n^3 + 1 + 3n^2 + 3n - n - 1$

$= (n^3 - n) + 3(n^2 + n)$

$= (n^3 - n) + 3(n^2 + n)$

The first term is divisible by the inductive hypothesis, The second term 3 times of an integer

Prove that $\sum_{i=1}^{n} 1 + 2 + 2^2 + \cdots + 2^n = 2^{n+1} - 1$

Basis step :- To show $P(1)$ is true.

$n = 1$

$1 + 2 = 2^{1+1} - 1$

$3 = 3$

Inductive step :-

$P(n)$ is true $1 + 2 + 3 \cdots + 2^n = 2^{n+1} - 1$

To show $P(n+1)$ is true

$1 + 2 + \cdots + 2^n + 2^{n+1} = 2^{n+1+1} - 1$

$2^{n+1} - 1 + 2^{n+1} = 2^{n+2} - 1$

$2 \cdot 2^{n+1} - 1 = 2^{n+2} - 1$

$2^{n+2} - 1 = 2^{n+2} - 1$

$\therefore P(n+1)$ is true.

Trees

Def (4) :- The set of rooted trees, where a rooted tree consists of a set of vertices containing a distinguished vertex called the root, & edges connecting these vertices can be defined recursively by these steps.

Basis step : A single vertex r is rooted tree

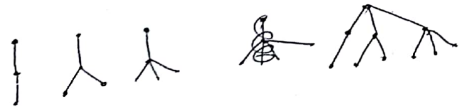
Recursive step :-

Suppose that $T_1, T_2, \ldots T_n$ are rooted trees with roots $r_1, r_2, \ldots r_n$ respectively. Then the graph starts from root 'r' which is not in rooted set. Then each $T_1, T_2, \ldots T_N$ are added to root through an edge

Basis :

Step (1)

Step (2)



Basis step :- If $w \in \Sigma^*$, then $w \cdot \lambda = w$, where λ is an empty string. (4)

Recursive Step :- If $w_1 \in \Sigma^*$ and $w_2 \in \Sigma^*$ and $x \in \Sigma$ then $w_1 \cdot (w_2 \cdot x) = (w_1 \cdot w_2) x$

Let $w_1 = CB$
$w_2 = IT$
$w_1 \cdot w_2 = CBIT$

→ Length of a string

Basis :- $l(\lambda) = 0$ (λ is an empty string)

$l(w) = w$
$l(wx) = w + 1$ ($\because x \in \Sigma, w \in \Sigma^*$)

→ well formed Formula consists of variables & numerals, operators from the set $\{+, -, *, /, \uparrow\}$ expression

(5) Basis :- x is wellformed, if x is numeral or variable

Recursive If F & G are well-formed, then (F+G), (F-G), (F*G), (F/G) and (F↑G) are well-formed formulas.

Def 0:- The set Σ^* of strings over the alphabet Σ can be defined recursively by

∴ Basis Step :- $\lambda \in \Sigma^*$ (where λ is the empty string containing no symbols)

∴ Recursive Step :- If $w \in \Sigma^*$ and $x \in \Sigma$, then $wx \in \Sigma^*$

(a) Consider the subset 'S' of the set of integers defined by

Basis Step :- $3 \in S$

Recursive step :- If $x \in S$, & $y \in S$, then $x+y \in S$

→ New elements found in S are.

3 → basis step

3+3 → 6 Ap① Recm

3+6 → 9

6+3 → 9

6+6 → 12

(b) Let 'S' be the the subset of ordered pairs of integers recursively defiey by

Basis Step :- $(0,0) \in S$

Inductive step :- If $(a,b) \in S$, then $(a, b+1) \in S$, $(a+1, b+1) \in S$ and $(a+2, b+1) \in S$

~~$S = \{(0,0), (0,1), (1,1), (3,3)\}$~~

Ind $(0,0) \in S$

$\forall S = a, b \in S$, $(a, b+1) \in S$, $(a+1, b+1) \in S$, $(a+2, b+1) \in S$

$S = \{(0,1), (1,1), \in (0,0)$

$= \{(0,1), (1,1), (2,1), (0,2), (1,2), (3,2)$
$(4,2), (0,3), (1,3) (3,3), (3,3) (4,3), (5,3)$
$(6,3) (0,4), (1,4), (3,4), (3,4), (4,4), (5,4),$
$(0,5), (1,5), (2,5), (3,5), (4,5), (5,5), (6,5)$
$(0,6), (6,4), (7,4), (8,4)\}$

(a) List the elements of 'S' produced by the first four application of the recursive definition

$S = \{(0,1) (1,1) (2,1)$
$(0,2) (1,2) (2,2) (3,2) (4,2)$
$(0,3) (1,3) (3,3) (4,3) (5,3) (6,3)$
$(0,4) (1,4) (2,4) (3,4)$
$(4,4) (5,4) (6,4) (7,4) (8,4)$

Def :- Two strings can be combined via the operation of concatenation. Let Σ be a set of symbols and Σ^* be the set of strings formed from symbols in Σ we can define the concatenation of two strings. denoted by '.' recursively

Unit-III

: Advanced Counting Techniques :

Many counting problems can be solved using formal power series called generating functions, where the co-efficients of powers of 'x' represent terms of the sequence, we are interested in.

Ex: The no. of bacteria in a colony double every hour, If a colony begin with five bacteria, how many will be present in n hours?

Let a_n be the no. of bacteria at the end of 'n' hours.

Becoz the no. of bacteria doubles every hour

$\therefore$ $\boxed{a_n = 2 \cdot a_{n-1}}$ initial condition $a_0 = 5$

If $n = 3$.

$a_3 = 2a_2$

$a_{2+1} = 2(a_1))$

$= 2(2(2(a_0)))$

$= 8a_0 = 8 \times 5 = 40$

10
20
to

Def: A recurrence relation for the sequence $\{a_n\}$ is a rule or an equation that expresses a_n in terms of one or more of the previous terms of the sequence, namely $a_0, a_1, \ldots a_{n-1}$, for all integers 'n' with $n \geq n_0$, where n_0 is a non-negative integer. A sequence is called a solution of a recurrence relation if its terms satisfy the recurrence relation.

(a) Let $\{a_n\}$ be a sequence that satisfies the recurrence relation $a_n = a_{n-1} + a_{n-2}$ for $n = 2, 3, 4 \ldots$ & Suppose that $a_0 = 3$ and $a_1 = 5$ what are a_2 and a_3?

Ah $a_2 = a_1 - a_0$

$= 5 - 3$

$= 2$

$a_3 = a_2 - a_1$

$= 2 - 5$

$= -3$

(a) Compound interest, Suppose that a person deposits \$10,000 in a saving account at a bank yielding 11% per year with interest compounded annually. How much will be in the account after 30.

Ah $P_n = P_{n-1} + 0.11 P_{n-1} = (1.11) P_{n-1}$

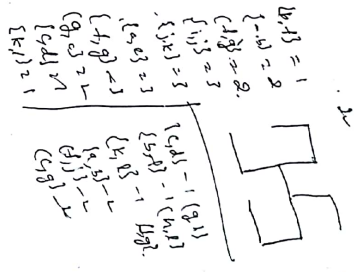
$P_1 = (1.11) P_0$

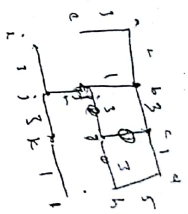
$P_2 = (1.11) P_1 = (1.11)^2 P_0$

$P_n = (1.11) P_{n-1} = (1.11)^n P_0$

$H_n = 2H_{n-1} + 1$

$P_{30} = (1.11)^{30} 10,000 =$





Applications of Congruences

Hashing functions – Records are identified using a key

Most Common Hash function ⇒ $h(k) = k \bmod m$

where 'm' is the no. of available memory locations.

Hashing function is not a one-to-one, more than one file may be assigned to a memory location when this happens, we say that a collision occurs.

→ one way to resolve a collision is to assign the first free location following the occupied.

Eg: $m = 111$

SSN = 064212848

$064212848 \bmod 111 = h(064212848) = 14$ → 14th location assigned.

$037149212 \bmod 111 = h(037149212) = 655$ → location assigned.

Ex $h(107405723) = 107405723 \bmod 111 = 14$,

14 already filled so is stored in next free location i.e., 15th location

1. Integers & Division

Number Theory = Integers + their properties.

Division Def

If a & b are integers with $a \neq 0$, we say that 'a divides b' if there is an integer 'c' such that $b = ac$. When 'a divides b' we say that 'a' is a factor of 'b' & 'b' is a multiple of 'a'.

The notation $a \mid b$ denotes that 'a divides b'.

We write $a \nmid b$ when a does not divide b.

Theorem 1:

Let a, b & c be integers, Then

1. If $a \mid b$ & $a \mid c$ then $a \mid (b+c)$;
2. If $a \mid b$ then $a \mid bc$ for all integer c;
3. If $a \mid b$ & $b \mid c$, then $a \mid c$.

④ A parking lot has 31 visitors spaces, numbered from 0 to 30, visitors are assigned parking spaces using first three digits on a visitor's license plates.

ⓐ What is the hashing function used? $h(k) = k \bmod 31$

ⓑ Which spaces are assigned by the hashing function to cars that have these first three digits on their license plates?

317 — 317 mod 31 = 7

918 — 918 mod 31 = 19

007 — 007 mod 31 = 7

100 — 100 mod 31 = 7

111 — 111 mod 31 = 18

310 — 310 mod 31 = 0.

$31 \times 29 = 899$

ⓒ Describe the a procedure visitors should follow to find a free parking space, when the space they are assigned is occupied.

→ Take the next available space (mod 31).

Pseudorandom Numbers :

→ Randomly chosen no.s are often needed for Computer Simulations. Different methods have been devised for generating no.s that have properties of randomly chosen no.s,

→ No.'s generated by Systematic methods are not truly random, they are called pseudorandom numbers.

Procedure to generate pseudorandom number

→ Pseudorandom numbers is the linear Congruential method

We choose four integers : the modulus 'm',
multiplier 'a',
increment 'c',
& Seed 'x_0'.

with $2 \le a < m$, $0 \le c < m$, & $0 \le x_0 < m$.

A Sequence of Pseudorandom no.'s $\{x_n\}$, with $0 \le x_n < m$ for all 'n'.

$$x_{n+1} = (ax_n + c) \bmod m$$

(a) $m = 9$, $a = 7$, $c = 4$ & $x_0 = 3$

The Sequence of pseudorandom no's generated by the

$x_{n+1} = (ax_n + c) \bmod m$

$x_1 = 7 \times 3 + 4 \bmod 9 = 25 \bmod 9 = 7$

$x_2 = 7x_1 + 4 \bmod 9 = 53 \bmod 9 = 8$

$x_3 = = 60 \bmod 9 = 6$

$x_4 = = 46 \bmod 9 = 1$

$x_5 = = 11 \bmod 9 = 2$

$x_6 = = 18 \bmod 9 = 0$

$x_7 = = 4 \bmod 9 = 4$

$x_8 = = 32 \bmod 9 = 5$

$x_9 = = 39 \bmod 9 = 3$

(b) what is the sequence of pseudorandom no.s is generated using the linear Congruential generator

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

(a = 4, c = 1, m = 7)

Ans $x_0 = 3$

$x_1 = 4 \times 3 + 1 \bmod 7 = 13 \bmod 7 = 6$

$x_2 = 4 \times 6 + 1 \bmod 7 = 24 \bmod 7 = 3$

$x_3 = 4 \times 3 + 1 \bmod 7 = 12 \bmod 7 = 5$

$x_4 = 4 \times 5 + 1 \bmod 7 = 20 \bmod 7 = 6$

$x_5 = 4 \times 6 + 1 \bmod 7 = 24 \bmod 7 = 3$

$x_6 = 4 \times 3 + 1 \bmod 7 = 22 \bmod 7 = 5$

$x_7 = 4 \times 5 + 1 \bmod 7 = 20 \bmod 7 = 6$

$x_0 = 2$

$x_{n+1} = 3x_n \bmod 11$

$x_1 = 6 \bmod 11 = 6$

$x_2 = 18 \bmod 11 = 7$

$x_3 = 21 \bmod 11 = 10$

$x_4 = 30 \bmod 11 = 8$

$x_5 = 24 \bmod 11 = 4$

$x_6 = 6 \bmod 11 = 6$

$x_7 = 18 \bmod 11 = 7$

$x_8 = 24 \bmod 11 = 4$

$x_9 = 30 \bmod 11 = 8$

$x_{10} = 24 \bmod 11 = 2$

Cryptology — involves study of secret messages.

Eg: B is sent ∈ } Encryption.
X ∧ ∧ A

Eg: A — 0
K — 10
Z — 25 —

Caesar's encryption method can be represented by a function assigning a non-ve integer 'p', $p \leq 25$

$f(p)$ in the set $\{0, 1, 2, \ldots 25\}$

with

$f(p) = (p+3) \bmod 26$

(a) What is the secret message for the message "HEET YOU IN THE CBIT".

12 4 4 19 | 24 14 20 | 8 13 | 19 7 4 | 2 1 9 8 19

$f(p) = (p+3) \bmod 26$

15 mod 26

15 7 7 22 | 1 17 -7 | 11 16 | 22 10 7 | 5 4 22

$f(p) = (p-3) \bmod 26$

To enhance this method

$f(p) = (ap + b) \bmod 26$

↓

a, b — int's

f is bijective

Affine Transformation

K = ?

$f(p) = (7p+3) \bmod 26$

$f(p) = (p+13) \bmod 26$

↓

INDIA IS MY COUNTRY

Representation Integers

Pf in (2n)

- Types of numbers based on base
  - Decimal
  - Binary
  - Octal
  - Hexadecimal

Algo:- ①

Constructing base-b Expansion (n): true if

```
q = n
k = 0
while q ≠ 0
begin  a_k = q mod b
       q = ⌊q/b⌋
       k = k+1
end  {the base b expansion of 'n' is (a_{k-1}, ..., a_1 a_0)_b}
```

Algo :- ②

Addition of Integers

Procedure add (a, b: +ve int)

{the binary expansion of 'a' & 'b' are $(a_{n-1}, a_{n-2}, \ldots, a_0)_2$ & $(b_{n-1}, b_{n-2}, \ldots, b_0)_2$ respectively.

```
c = 0
for j = 0 to n-1
begin
    d = ⌊(a_j + b_j + c)/2⌋
    s_j = a_j + b_j + c - 2d
    c = d
end
s_n = c
```

{the binary expansion of the sum is $(s_n s_{n-1} \ldots s_0)$}

1001

j = 0 to 3

j = 0: $d = \lfloor 0+1+0/2 \rfloor = 0$, $s_0 = 0+1+0-2\times0 = 1$, $c = 0$

j = 1: $d = \lfloor 0+1+0/2 \rfloor = 1$, $s_1 = 1+1+0-2\times1 = 0$, $c = 1$

$s_1 = 0$

$s_0 = 1$

GIL

a_n = 1110

b_n = 1011

11001

j = 2: $d = \lfloor 1+0+1/2 \rfloor = 1$, $s_2 = 1+0+1-2 = 0$, $c = 1$, $s_2 = 0$

j = 3: $d = \lfloor 1/2 \rfloor = 1$, $c_3 = 3-2 = 1$, $c = 1$, $s_3 = 1$

Algo 1: Multiplying Int's

Procedure: multiply (a, b : +ve int)

{ the binary expan of a & b are

for j=0 to n-1

begin

if b_j=1 then c_j = a shifted 'j' times

else c_j = 0

end

{ $c_0, c_1, \ldots, c_{n-1}$ are the partial products }

p := 0

for j=0 to n-1

p = p + c_j

{ p = ab }

Algorithm ④ : Computing div & mod

procedure division algorithm (a: integer, d: positive integer)

q = 0

r = |a|

while r ≥ d

begin

r = r - d

q = q + 1

end

if a < 0 and r > 0 then

begin r = d - r

end q = -(q+1)

{ q = a div d is the quotient
r = a mod d is the remainder }

Algo 5: Modular Exponentiation

Procedure modular exponentiation (b: integer, n = $(a_{k-1}, a_{k-2}, \ldots, a_0)_2$,
m : positive integer)

x = 1

power = b mod m

for i = 0 to k-1

begin if a_i = 1 then x = (x . power) mod m

power = (power . power) mod m

end

{ x equals b^n mod m }

⑤ Use the algorithm 5 to find 123^{1001} mod 101

$(1001)_{10} = (1111101001)_2$

x = 1 Power = 123 mod 101 = 22

i=0 a_0=1 x = (1 . 22) mod 101 = 22 Power = 22^2 mod 101 = 484 mod 101 = 81

i=1 a_1=0 x = 22 Power = $\frac{6400}{80 \times 80}$ mod 101 = 37

i=2 a_2=0 x = 22 Power = $\frac{37 \times 37}{1369}$ mod 101 = 56

i=3 a_3=1 x = $\frac{(22 \times 56)}{1232}$ mod 101 = 20 Power = $\frac{56 \times 56}{3136}$ mod 101 = 5

i=4 a_4=0 x = 20 Power = 5 mod 101 = 5

i=5 a_5=1 x = 100 mod 101 = 1 Power = 25 mod 101 = 25

i=6 a_6=1 x = 25 mod 101 = 25 Power = $\frac{25 \times 25}{625}$ mod 101 = 19

i=7 a_7=1 x = $\frac{19 \times 25}{475}$ mod 101 = 71 Power = $\frac{19^2}{361}$ mod 101 = 58

i=8 a_8=1 x = $\frac{71 \times 58}{4118}$ mod 101 = 78 Power = $\frac{58^2}{3364}$ mod 101 = 31

i=9 a_9=1 x = $\frac{78 \times 31}{2418}$ mod 101 = 97

The Euclidean Algorithm:

Used to find gcd.

gcd (91, 287) ⇒ 287 = 91.3 + 14

Lemma ①:- Let $a = bq + r$, where a, b, q & r are integers.

Then $\boxed{\gcd(a,b) = \gcd(b,r)}$

Euclidean Algorithm

```
procedure gcd (a,b: +ve integers)
    x = a
    y = b
    while y ≠ 0
    begin
        r = x mod y
        x = y
        y = r
    end {gcd(a,b) is x}
```

② Find the gcd of 414 & 662

$662 = 414.1 + 248$

$414 = 248.1 + 166$

$248 = 166.1 + 82$

$166 = 82.2 + 2$

$82 = 2.41$

p – 36, 38, 44, 52, 58, 40.

89
194
73

1, 2, 5, 6, 7, 8, 10, 15,
17, 18, 19, 20, 22, 26,
31, 33, 33 – 17

p – 301, 51, 59, 53 16

p – 309, 310, 306

29

92

Euclidean Algorithm

Efficient method for finding the greatest common divisor, called the Euclidean Algorithm.

Def :- Let 'a' & 'b' be integers, not both zero. The largest integer 'd' such that $d|a$ and $d|b$ is called the greatest common divisor of 'a' & 'b'. The greatest common divisor of 'a' & 'b' is denoted by gcd (a,b).

Lemma – Let $a = bq + r$, where a, b, q & 'r' are integers.

Then $\boxed{\gcd(a,b) = \gcd(b,r)}$

Algorithm ⑥ The Euclidean Algorithm

```
Procedure gcd (a,b: +ve integers)
    x = a
    y = b
    while y ≠ 0
    begin
        r = x mod y
        x = y
        y = r
    end {gcd(a,b) is x}
```

414 & 662

x = 662	419	248
y = 414	248	166
r = 662 mod 414 = 248	r = 414 mod 248 = 166	r = 248 mod 166 = 82
x = 419	x = 248	x = 166
y = 248	y = 166	y = 82

166	82
82	2
r = 2	r = 0
x = 82	(x = 2)
y = 2	y = 0

Applications of Number Theory

① gcd (a,b) can be expressed as linear combination

Theorem If 'a' & 'b' are positive integers, then there exist integers 's' & 't' such that gcd (a, b) = sa + tb.

It is called as **Extended Euclidean Algorithm.**

② Express gcd (252, 198) = 18 as a linear combination of 252 & 198

$252 = 1 \times 198 + 54$ — ①

$198 = 3 \times 54 + 36$ — ②

$54 = 1 \times 36 + 18$ — ③

$36 = 2 \times 18$ — ④

Using the next-to-last division

$18 = 54 - 1 \times 36$ — ⑤

$36 = 198 - 3 \times 54$ — ⑥

Substitute ⑥ in ⑤.

$18 = 54 - 1 \times (198 - 3 \times 54)$

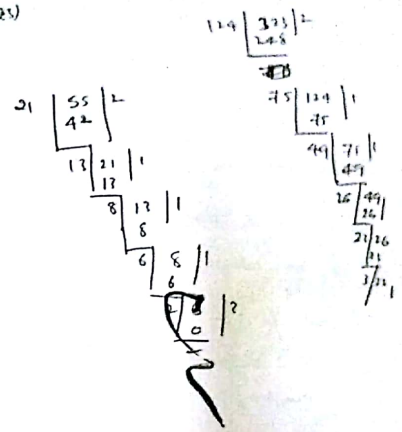
$= 4 \times 54 - 1 \times 198$

$= 4 \times (252 - 1 \times 198) - 1 \times 198$

$18 = 4 \times 252 - 4 \times 198$

③ gcd (124, 323)

55, 21



$55 = 21 \times 2 + 13$ — ①

$21 = 1 \times 13 + 8$ — ②

$13 = 1 \times 8 + 5$ — ③

$8 = 1 \times 5 + 3$ — ④

$5 = 1 \times 3 + 2$ — ⑤

$3 = 1 \times 2 + 1$ — ⑥

$2 = 2 \times 1 + 0$ — ⑦

from ⑥

$1 = 3 - 1 \times 2$

$1 = 3 - 1 \times (5 - 1 \times 3)$ from ⑤ $2 =$

$= 2 \times 3 - 1 \times 5$

$= 2(8 - 1 \times 5) - 1 \times 5$ from ④ $3 =$

$= 2 \times 8 - 3 \times 5$

$= 2 \times 8 - 3 \times (13 - 1 \times 8)$ from ③

$= 5 \times 8 - 3 \times 13$

$= 5 \times (21 - 1 \times 13) - 3 \times 13$ from ②

$= 5 \times 21 - 8 \times 13$

$= 5 \times 21 - 8 \times (55 - 2 \times 21)$ from ①

$= 21 \times 21 - 8 \times 55$

→ If $a, b, \& c$ are +ve integers such that $\gcd(a,b)=1$ and $a \mid bc$, then $a \mid c$.

→ If 'p' is a prime and $p \mid a_1 a_2 \cdots a_n$, where each a_i is an integer, then $p \mid a_i$ for some 'i'.

→ Let 'm' be a +ve integer & let $a, b \& c$ be integers If $ac \equiv bc \pmod m$ and $\gcd(c,m) \equiv 1$ then $a \equiv b \pmod m$

Linear Congruences

→ A congruence of the form

$$\boxed{ax \equiv b \pmod m}$$

where 'm' - +ve integer

a, b - integers

x - variable. is called linear congruence.

If $\bar{a}a \equiv 1 \pmod m$ exists the $\bar{a}$ is inverse of a modulo m.

Theorem: If 'a' & 'm' are relatively prime integers & $m>1$, then an inverse of $a \bmod m$ exists. Further this inverse is unique modulo 'm' (i.e, there is a unique +ve integer $\bar{a} < m$ i.e. an inverse of $a \bmod m$ & every other inverse of $a \bmod m$ is congruent to $\bar{a} \bmod m$)

Theorem ① $\gcd(a,m)=1$ then there is an integers s & t such that $sa+tm=1$

$\Rightarrow sa+tm \equiv 1 \pmod m$

$\because tm \equiv 0 \pmod m$ it follows that

$sa \equiv 1 \pmod m \longrightarrow \therefore s$ inverse of $a \bmod m$

ⓐ Find the inverse of $3 \bmod 7$.

$\gcd(3,7)=1 \therefore$ inverse of $3 \bmod 7$ exists

$$\begin{array}{r|l} 3 & 7 \\ & 6 \\ \hline 1 & 3 \\ & 1 \\ \hline & 0 \end{array} \quad \begin{array}{l} 2 \\ \\ 1 \\ \\ \end{array}$$

$7 = 2 \times 3 + 1 \quad -①$

for ① $\quad -2 \times 3 + 1 \times 7 = 1$

this is $sa + t \times m = 1$.

-2 is inverse $3 \bmod 7$.

ⓑ What are the solutions of linear congruence $3x \equiv 4 \pmod 7$

Ans By the above '-2' is inverse of $3 \bmod 7$

$-2 \times 3x \equiv -2 \times 4 \pmod 7$

-6

(multiply with 2)

$3x \equiv 4 \bmod 7$

$\gcd(3,7)=1 \Rightarrow 7 = 2 \cdot 3 + 1$

$-2 \cdot 3 + 7 \cdot 1 = 1$

$sa + tm = 1$

$\therefore -2$

⑦ Find the inverse of 3 modulo 7.

Sol: $\gcd(3,7) = 1$ ∴ Inverse of 3 mod 7 exists.

From Euclidean.

$7 = 2.3 + 1$

$3 = 3.1 + 0$

$1 =$

From extended Euclidean

$\Rightarrow \quad 1 = -2.3 + 7 \times 1$

From the above theorem

3 mod 7 $\quad 1 = -2 \times 3 + 7 \times 1$

s a + m t

-2 is inverse of 3 mod 7

s " " a mod m

∴ -2 is inverse of 3 mod 7.

$x \equiv -2 \bmod 7$ is also inverse of 3

Ex: $5 \equiv -2 \bmod 7$, $-9, 12, \ldots$

⑧ What are the solutions of $3x \equiv 4 \pmod 7$? — the linear congruence

A: From above -2 is inverse of 3 mod 7

Multiply both sides of the congruence by -2

$-2 \times 3x \equiv -2 \times 4 \pmod 7$

⑨ Solve $3x \equiv 4 \pmod 7$

-2 is inverse of 3 mod 7

Multiply both sides with -2

$-2 \times 3x \equiv -2 \times 4 \pmod 7$

$-6.x \equiv -8 \pmod 7$

Apply mod 7

$-6 \pmod 7 \times x \equiv -8 \pmod 7$

$1.x = 6 \pmod 7$

$x = 6$

Check

$3 \times 6 \equiv 4 \pmod 7$

$18 \equiv 4 \pmod 7$ ✓

Check

L.H.S: 3×6 (18)

R.H.S: 4 mod 7

Apply mod 7

$4 = 4$

If $8 \bmod 5 = 3$
$8 \equiv 3 \bmod 5$

If $-8 \bmod 5 = 2$
$-8 \equiv 2 \bmod 5$

If $-2 \bmod 9 = 7$
$-2 \equiv 7 \pmod 9$

If $25 \bmod 2 = 1$
$25 \equiv 1 \bmod 2$.

(2) $19x \equiv 4 \pmod{141}$

Find inverse.

$\gcd(19, 141) = 1$

∴ inverse exists

$141 = 19 \times 7 + 8$
$19 = 8 \times 2 + 3$
$8 = 3 \times 2 + 2$
$3 = 2 \times 1 + 1$

19 mod 141

19	141 / 133	7
5	19 / 16	2
3	8 / 6	2
2	3 / 2	1
1	2 / 2	2
	0	

$1 = 3 - 2 \times 1$
$1 = 3 - (5 - 3 \times 2)$
$= 3 \times 3 - 5 \times 1$
$= 3 \times (19 - 8 \times 2) - 8 \times 1$
$= 3 \times 19 - 8 \times 7$
$= 3 \times 19 - (141 - 19 \times 7) \times 7$

$1 = 52 \times 19 - 7 \times 141$

satisfy

$8 \bmod 5 = 3$
$8 \equiv 3 \bmod 5$
$-8 \bmod 5 = 2$.
$-8 \equiv 2 \bmod 5$
$12 \bmod 9 = 3$
$12 \equiv 3 \pmod 9$

$-2 \bmod 9 = 7$
$-2 \equiv 7 \pmod 9$
$25 \bmod 2 = 1$
$25 \equiv 1 \bmod 2$

$-8 \equiv 6 \bmod 7$
$-8 \bmod 7 = -1$
52×19
468
51
988

Also $19x \equiv 4 \pmod{141}$

Inverse of 19 mod 141 is 52

multiply with 52

$19 \times 52\, x \equiv 52 \times 4 \pmod{141}$
$52 \times 19 \times x \equiv 208 \pmod{141}$ (mod 4)
$\vee$
$988 \pmod{141} = 1$

$1 \cdot x \equiv 208 \pmod{141}$
$x \equiv \frac{208}{141} \pmod{141}$
$x = 67 \pmod{141}$

$x = 67$

$-2 \times 3x \equiv -2 \times 4 \pmod 7$
$(-6 \bmod 7) = 1$
$1 \cdot x = 6 \pmod 7$.
$x = 6$

~~$(-6 \bmod 7) =$~~ (24)
$(18 \bmod 7) = 4$
$4 \equiv 4$

$\Rightarrow 19x = 4 \pmod{141}$ $\Rightarrow$

LHS: $19 \times x$, 19×67, $1273 \bmod 141 = 4$
RHS: $4 \pmod{141}$

Check

$19x \equiv 4 \pmod{141}$
$19 \times 67 \equiv 4 \pmod{141}$
$(1273) \bmod 141 = 4$

Chaitanya Bharathi Institute of Technology, Hyderabad-75

Alumni Survey Form

(B.E.-IT)

Name: Year of Graduation:

Organization with address:

Phone: E-Mail:

The purpose of this questionnaire is to solicit, in a completely confidential manner, information about your satisfaction with your experience of graduate education at CBIT and your professional activities since you have completed your graduate degree. Now that some time has passed since you have completed your degree, we would like you to tell us how well your graduate training has served you. Your responses will help us improve and strengthen graduate education at both the departmental and Institution levels, as well as strengthens our relationship with our graduate. Thank you in advance for your cooperation and participation.

How would you assess each of the following aspects of your experiences at CBIT?	Excellent	Very Good	Good	Fair	Poor
Overall academic experiences at CBIT					
Overall academic experience in your department or program					
Co-curricular/Extra-curricular activities (NSS, others) at CBIT					

Since completing your CBIT degree, have you or are you planning to enroll in any other advanced degree programs?

Institution at which you enrolled	Field of specialization	Year in which you began the program	Year in which you completed the program

Please list down your employment details

$19 \times 24\, x \equiv 24 \times 44 \pmod{191}$

$456\, x \pmod{191} \equiv 96$

$33\, x = 96$

Chinese Reminder Theorem

what are the solutions of the system of congruences

$x \equiv 2 \pmod 3$
$x \equiv 3 \pmod 5$
$x \equiv 2 \pmod 7$ → done by chinese remainder

Chinese Reminder Theorem

Let $m_1, m_2 \dots m_n$ be pairwise relatively prime +ve integers and $a_1, a_2 \dots a_n$ arbitrary integers. Then the system

$x \equiv a_1 \pmod{m_1}$
$x \equiv a_2 \pmod{m_2}$
$\vdots$
$x \equiv a_n \pmod{m_n}$

has unique solution $m = m_1, m_2 \dots m_n$ (i.e, there is a solution x with $0 \le x < m$ & all other solutions are congruent modulo m to this solution)

→ To construct simultaneous solution

find $M_k = m/m_k$

$M_k y_k \equiv 1 \pmod{m_k}$

$x = a_1 M_1 y_1 + a_2 M_2 y_2 + \cdots + a_n M_n y_n$

$x \equiv a_k M_k y_k \equiv a_k \pmod{m_k}$

(1) Solve the System of Congruences

$x \equiv 2 \pmod 3$

$x \equiv 3 \pmod 5$

$x \equiv 2 \pmod 7$

Sol:

Let $m = 3 \times 5 \times 7 = 105$

$M_1 = \frac{m_3}{m_k} \Rightarrow M_1 = \frac{105}{3} = 35$

$M_2 = \frac{105}{5} = 21$

$M_3 = \frac{105}{7} = 15$

$35 \equiv 2 \pmod 3$

$M_1 = 35 \bmod 3 \Rightarrow 2$

$21 \equiv 1 \pmod 5$

$M_2 = 21 \bmod 5 \Rightarrow 1$

$15 \equiv 1 \pmod 5$

$M_3 = 15 \bmod 7 \Rightarrow$

$35 =$

$35 x y \equiv 1 \pmod 3$

$x \equiv a_1 M_1 y_1 + a_2 M_2 y_2 + a_3 M_3 y_3$

$= 2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1$

$= 140 + 63 + 30$

$= 233 \bmod 105)$

$x \equiv$

140
63
30
233

$233 \equiv 23 \bmod 105$ $(373 \bmod 105)$

a_1 is smaller the no. $23 \bmod 3 = 2$ $23 \bmod 7 = 2$

(6). $x \equiv 1 \pmod 2$

$x \equiv 2 \pmod 3$

$x \equiv 3 \pmod 5$

$x \equiv 4 \pmod{11}$

$m = 2 \times 3 \times 5 \times 11 = 330$

$M_1 = \frac{330}{2} = 165$

$M_2 = \frac{330}{3} = 110$

$M_3 = \frac{330}{5} = 66$

$M_4 = \frac{330}{11} = 30$

$165 \bmod 2 \Rightarrow 165 \equiv 1 \pmod 2$

$110 \bmod 3 \Rightarrow 110 \equiv 2 \pmod 3$

$66 \bmod 5 \Rightarrow 66 \equiv 6 \pmod 5$

$30 \bmod 11 \Rightarrow 30 \equiv 8 \pmod{11}$

$x \equiv 1 \times 165 \times 1 + 2 \times 110 \times 2 + 3 \times 66 \times 6 + 4 \times 30 \times 8$

$= 165 + 440 + 1188 + 960$

$\equiv 2753 \bmod 330$

$2753 \equiv 113 \pmod{330}$

$113 \equiv 1 \pmod 2$

$113 \equiv 2 \pmod 3$

$113 \equiv 3 \pmod 5$

$113 \equiv 4 \pmod{11}$

Fermat's Little Theorem

If 'p' is prime & 'a' is an integer not divisible by 'p' then

$$a^{p-1} \equiv 1 \pmod{p}$$

for every integer 'a'

we have $\boxed{a^p \equiv a \pmod{p}}$

⇒ Let 'b' be a +ve integer. If 'n' is a composite +ve integer and $b^{n-1} \equiv 1 \pmod{n}$, then 'n' is called a pseudoprime to the base 'b'.

⇒ A Composite integer 'n' that satisfies the congruence $b^{n-1} \equiv 1 \pmod{n}$ for all the integers 'b' with $\gcd(b,n)=1$ is called Carmichael no.

(a) $x \equiv 2 \pmod 3$ To find solution

$M = m_1 \cdot m_2 \cdot m_3 \cdots m_k$ $\quad M_\gamma = \frac{M}{m_\gamma}$

$\gcd(M_\gamma, m_\gamma) = 1$

Let there is a unique soln.

$M_\gamma x \equiv 1 \pmod{m_\gamma}$.

$\therefore \quad M_\gamma x_\gamma \equiv 1 \pmod{m_\gamma}$.

Let us consider a solution

$x' = a_1 M_1 x_1 + a_2 M_2 x_2 + \cdots + a_k M_k x_k$

$\therefore$ unique soln $x \equiv a_k M_k y_k \equiv a_k \pmod{m_k}$

(a) $x \equiv 2 \pmod 3$, $x \equiv 4 \pmod 5$ $x \equiv 5 \pmod 7$

$m_1 = 3$, $m_2 = 5$, $m_3 = 7$

$a_1 = 2$, $a_2 = 4$, $a_3 = 5$

$M = 3 \times 5 \times 7 = 105$

$M_1 = \frac{M}{3} = 35$ $\quad M_2 = \frac{105}{5} = 21$ $\quad M_3 = \frac{105}{7} = 15$.

$M_r x_r \equiv 1 \pmod{n_r}$, $r = 1, 2, 3$.

$35x_1 \equiv 1 \pmod 3$, $21x_2 \equiv 1 \pmod 5$, $15x_3 \equiv 1 \pmod 7$ (1)

$35x_1 \equiv 1 \pmod 3$

$x = 0, 1, 2$

$x_1 = 2$.

$21x_2 \equiv 1 \pmod 5$

$x = 0, 1, 2, 3, 4$

$x_2 = 1$

$15x_3 \equiv 1 \pmod 7$

$x = 0, 1, 2, 3, 4, 5, 6$.

$x_3 = 1$

$x' = a_1 M_1 x_1 + a_2 M_2 x_2 + \cdots$

$= 2 \times 35 \times 2 + 4 \times 21 \times 1 + 5 \times 15 \times 1 \pmod{105}$

$= 140 + 84 + 75 \pmod{105}$.

$x' \equiv 299 \pmod{105}$. (2)

$\Rightarrow$ 89 is uni

rem 2 | 3, rem 4 | 5, rem 5 | 7

Applications of Number Theory

In addition to generation of random no.'s & stuff ciphers, developing some key results & presenting two important applications,

1) A method for performing arithmetic with large integers
2) A Public Key System.

Theorem ① extended Euclidean Algorithm

If 'a' and 'b' are +ve integers, then there exist integers 's' and 't' such that $\gcd(a, b) = sa + tb$.

Express $\gcd(252, 198) = 18$ as a linear combination of 252 and 198.

To show that $\gcd(252, 198) = 18$, the Euclidean algorithm uses these divisions:

$$252 = 1 \cdot 198 + 54 \quad — ①$$
$$198 = 3 \cdot 54 + 36 \quad — ②$$
$$54 = 1 \cdot 36 + 18 \quad — ③$$
$$36 = 2 \cdot 18 + 0 \quad — ④$$

30

198 | 252 | 1
198

54 | 198 | 3
162

36 | 54 | 1
36

18 | 36 | 2
36

0

from step ③

$$18 = 54 - 1 \times 36 \quad — ⑤$$

step ② $\quad 36 = 198 - 3 \times 54 \quad — ⑥$

Substitute ⑥ in ⑤

$$18 = 54 - 1 \times (198 - 3 \times 54) \quad — ⑦$$

take ① in ⑦

$$18 = (252 - 1 \times 198) - (1 \times 198 + 3 \times 54)$$

from ③ $18 = 54 - 1 \times 36$ — ④

from ② $36 = 198 - 3 \times 54$ — ⑥

$18 = 54 - 1 \times 36$

$= 54 - 1 \times (198 - 3 \times 54)$

$= 54 - 1 \times 198 + 3 \times 54$

$18 = 4 \times 54 - 1 \times 198$ — ⑦

from ①

$54 = 252 - 1 \times 198$ — ⑧

Substitute ⑧ in ⑦

$18 = 4 \times (252 - 1 \times 198) - 1 \times 198$

$18 = 4 \times 252 - 5 \times 198$

Proved.

gcd (252, 198) = 18

④ If a, b, and c are the integers such that gcd(a,b)=1 and a|bc, then a|c.

⑤ Express the gcd of each of these pairs of integers as a linear combination of these integers

⑧ (34, 55)

34	55	1
	34	
21	34	1
	21	
13	21	1
	13	
8		1

gcd(34,55)=1

2	2	1
1	2	2

gcd (34, 55)

① $55 = 1 \times 34 + 21$

② $34 = 1 \times 21 + 13$

③ $21 = 1 \times 13 + 8$

④ $13 = 1 \times 8 + 5$

⑤ $8 = 1 \times 5 + 3$

⑥ $5 = 1 \times 3 + 2$

⑦ $3 = 1 \times 2 + 1$

⑧ $2 = 1 \times 2 + 0$

from ⑦ ⑥

$3 = 12 - 1 \times 9$ — ⑦

from ④

$3 = 12 - 1 \times (21 - 1 \times 12)$

$= 2 \times 12 - 1 \times 21$ — ⑧

from ③ substitute 12 value

$3 = 2 \times (96 - 4 \times 21) - 1 \times 21$

$= 2 \times 96 - 5 \times 21$ — ⑨

from ② substitute 21 value in ⑨

$3 = 2 \times 96 - 5 \times (117 - 1 \times 96)$

$= 2 \times 96 - 5 \times 117 + 5 \times 96$

$= 7 \times 96 - 5 \times 117$ — ⑩

from ①

$3 = 7 \times (213 - 1 \times 117) - 5 \times 117$

$= 7 \times 213 - 12 \times 117$

⑨ gcd (48, 36)

① $213 = 1 \times 117 + 96$ — ①

② $117 = 1 \times 96 + 21$ — ②

③ $96 = 4 \times 21 + 12$ — ③

④ $21 = 1 \times 12 + 9$ — ④

⑤ $12 = 1 \times 9 + 3$ — ⑤

⑥ $9 = 3 \times 3 + 0$ — ⑥

$3 = 1 \cdot 213 + (-20) \cdot 117$

$3 = 12 \cdot 1 \times 9$

$3 = 12 \cdot (21 - 1 \times 12)$

$3 = 12 \cdot 21 - 1 \times 12$

① gcd (48, 36)

② $48 = 36 \times 1 + 12$ — ①

$36 = 3 \times 12 + 0$ — ②

from ①

$12 = 48 - 1 \times 36$

from ②

$12 = 1 \cdot (48) + (-1) \cdot 36$

If p is a prime and $p \mid a_1 a_2 \cdots a_n$ where each a_i is an integer, then $p \mid a_i$ for some i.

Theorem 2

Let m be a the integer and let a, b and c be inte

If $ac \equiv bc \pmod m$ and $\gcd(c, m) = 1$, then

$a \equiv b \pmod m$.

$ac \equiv bc \pmod m$,

$m \mid ac - bc = c(a-b)$

$\gcd(c, m) = 1 \Rightarrow m \mid a-b$.

Linear Congruences

A Congruence of the form

$$ax \equiv b \pmod m$$

where m is a the integer, a and b are integers, and x is a variable, is called a "linear Congruence".

Theorem 3

If a and m are relatively prime integers and m then an inverse of a modulo m exists. Furthermore this inverse is unique modulo m.

Proof: By theorem 1, because $\gcd(a, m) = 1$, there are integers s

$sa + tm = 1$

$\Rightarrow sa + tm \equiv 1 \pmod m$

Because $tm \equiv 0 \pmod m$,

$sa \equiv 1 \pmod m$ $\therefore$ s is an inverse of a modulo m

1) Find an inverse of

$\gcd(3, 7) = 1$ from theorem 3 tells us that an inverse of 3 modulo 7 exists

$7 = 2 \cdot 3 + 1$ — (1)

$(3 \bmod 7) \equiv (-2 \bmod 7)$

$3 \equiv -2$

From this (1)

$-2 \cdot 3 + 1 \cdot 7 = 1$

$sa + tm = 1$

$\therefore -2$ is an inverse of 3 modulo 7.

2) S.T. 15 is an inverse of 7 mod 26

$26 = 3 \cdot 7 + 5$ — (1)

$7 = 1 \cdot 5 + 2$ — (2)

$5 = 2 \cdot 2 + 1$ — (3)

$\gcd(7, 26) = 1$ $\therefore$ inverse exists.

$5 = 2 \times 2 + 1$ from (3)

$=$

$\gcd(26, 7) = 1$

$26 = 3 \cdot 7 + 5$ — (1)

$7 = 1 \times 5 + 2$ — (2)

$5 = 2 \times 2 + 1$ — (3)

$1 = 5 - (2 \times 2)$

$= 5 - 2(7 - 1 \times 5)$

$= 3 \times 5 + 2 \times 7$

$= 3 \times (26 - 3 \times 7) - 2 \times 7$

$1 = 3 \times 26 - 11 \times 7$

$15 \times 7 = 105$

$15 \cdot 7 \equiv 1 \pmod{26}$

$s \cdot a \equiv 1 \pmod m$

$\therefore$ s is the inverse of $a \bmod m$

$\therefore$ 15 is the inverse of $m \cdot 7 \bmod 26$

(1) gcd (141, 19)

$141 = 7 \times 19 + 8$
$19 = 2 \times 8 + 3$
$8 = 2 \times 3 + 2$
$3 = 1 \times 2 + 1$

$1 = 3 - 1 \times 2$
$= 3 - 1 \times (8 - 2 \times 3)$
$= 2 \times 3 - 1 \times 8$
$= 3(19 - 2 \times 8) - 1 \times 8$
$= 3 \times 19 - 7 \times 8$
$= 3 \times 19 - 7(141 - 7 \times 19)$
$1 = 52 \times 19 - 7 \times 141$

$= \frac{52}{2}$

(141 mod 19)

19 mod

(4) inverse of 3 mod 7

gcd (7, 3) = 1

$7 = 2 \times 3 + 1$
$1 = 7 - 2 \times 3$

$26 = 7 \times 3 + 5$
$7 = 5 \times 1 + 2$
$5 = 2 \times 2 + 1$
$2 = 1 \times 2 + 0$

from (1)
$1 = 5 - 2 \times 2$
(2) $1 = 5 - 2 \times (7 - 5)$
$= 3 \times 5 - 2 \times 7$
$= 3 \times (26 - 7 \times 3) - 2 \times 7$
$= 3 \times 26 - 11 \times 7$
$5a + 1 \equiv 6$

418
52
288

67 × 19
603
64
19 × 7

141) 208 (1
141
67

"a modulo m"

Linear Congruences

Proof (1) :- The linear congruence $ax \equiv b \pmod m$ has a solution if and only if $ax = b + km$

Theorem :
For the linear congruence $ax \equiv b \pmod m$, there exists no solutions if $\gcd(a,m) \nmid b$. If $\gcd(a,m) \mid b$, then there are exactly (a,m) solutions.

Proof (2) If $\gcd(a,m) \nmid b$, then $ax \equiv b \pmod m$ has no solutions.

(3) Does $3x \equiv 4 \pmod 9$ have any solutions?

Here $a=3$, $m=9$ $\gcd(a,m) = (3,9) = 3$

from proof (2) $\gcd(a,m) = 3 \nmid 4$

∴ No Solutions.

Does $2x \equiv 4 \pmod 6$ have any solutions?

$a=2$, $m=6$ $\gcd(2,6) = 2 \mid$

$2 \mid 4$ ∴ there exists a solution

Proof (1) ⊥ If $\gcd(a,m)=1$, then linear Congruence $ax \equiv b \pmod m$ has exactly one solution

(2) ⊥ If $(a,m) \mid b$, then $ax \equiv b \pmod m$ has exactly (a,m) Solutions

(12) What are the solutions of the linear congruence

$3x \equiv 4 \pmod 7$?

We know that $\gcd(3,7) = 1$ (invertible) $= -2$

multiply both sides with -2

$-2 \cdot 3x \equiv -2 \cdot 4 \pmod 7 \Rightarrow -6 \cdot x \equiv -8 \pmod 7$

$-6 \pmod 7 = 1$, $x = 6$

$\therefore -6 \equiv 1 \pmod 7$

$-8 \equiv 6 \pmod 7$

$x \equiv -8 \equiv 6 \pmod 7$

every x with $x \equiv 6 \pmod 7$ has a solution $\neq$ mod

$3x = 3 \times 6 = 18 \equiv 4 \pmod 7$

$x \equiv \boxed{x \equiv 6 \pmod 7}$

$6, 13, 20, \ldots \mid -1, -8, -15, \ldots$

(13) Solve $19x \equiv 4 \pmod{141}$ — (1)

Inverse of $19 \bmod 141 = 52$.

mod apply both side. multiply with 52

$52 \times 19x \equiv 52 \times 4 \pmod{141}$

$52 \times 19x = 208 \pmod{141}$

$988 \pmod{141} = 1 \times x = 67$

$x \equiv 67 \bmod 141$

$8 \bmod 5 = 3$

$8 \equiv 3 \pmod 5$

$-2 \bmod 9 = 7$

$-2 \equiv 7 \pmod 9$

$25 \bmod 2 = 1$

$25 \equiv 1 \pmod 2$

Check

$x = 67$

$192 \equiv 4 \pmod{141}$

$19 \times 67 = 4 \pmod{141}$

$1273 \equiv 4 \pmod{141}$

$1273 \bmod 141 = 4$

$19x \equiv 4 \pmod{141}$

L.H.S $= 4$ R.H.S

$19 \times 67 = 4$

$1273 \bmod 141$

$4 = 4$

If n_1, n_2, n_k are the integers that are pairwise coprime & $a_1, a_2 \ldots a_k$ are any integers, then Ch. R.T. is used to find the values of 'x' that solves the following congruences simultaneously

$x \equiv a_1 \pmod{n_1}$, $x \equiv a_2 \pmod{n_2}$ — $x \equiv a_3 \pmod{n_3}$

$x \equiv a_k \pmod{n_k}$

Value of 'x' is congruent to

$x' \; (a_1 m_1 y_1 + a_2 m_2 y_2 + a_3 m_3 y_3 + \cdots + a_k m_k y_k) \bmod M$

where $M = m_1 m_2 \cdots m_k$.

$\boxed{m_i = M/n_i}$ &

one of 'x' $\boxed{m_i y_i \equiv 1 \pmod{n_i}}$

A bag has certain no. of pens. If you take out 3 pens at a time, 2 pens are left, if you take out 4 pens at a time, 1 pen is left & if you take out 5 pens at a time 3 pens are left in the bag.
what is the smallest no. of pens in the bag?

$x \equiv 2 \pmod 3$ $x \equiv 1 \pmod 4$ $x \equiv 3 \pmod 5$

$a_1 m_1 y_1 + a_2 m_2 y_2 + a_3 m_3 y_3$

$2 \times 20 \times y_1 + 1 \times 15 \times y_2 + 3 \times 12 \times y_3$ — (1)

$M_1 = \frac{180}{3} = 60$, $M_2 = 240$, $M_3 = 300$

$m_i y_i \equiv 1 \pmod{n_i}$

$m_1 y_1 \equiv 1 \pmod{n_1}$

$20 \times y_1 \equiv 1 \pmod 3$

$20 \bmod 3 = 2 \Rightarrow 2 \times y_1 \equiv 1 \pmod 3$

$x \bmod 3 = 1 \Rightarrow$ multiply with 2

$4 \times y_1 = 2 \pmod 3$

$y_1 = 2 \pmod 3$

$m_1 y_1 \equiv 1 \pmod 4$

$15 y_1 \equiv 1 \pmod 4$

is mod 4 = 3

$3 y_1 \equiv 1 \pmod 4$

multiply both sides by 3

$9 y \equiv 3 \pmod 4$

$\boxed{y_1 \equiv 3 \pmod 4}$

$m_2 y_2 \equiv 1 \pmod 7$

$12 y_2 \equiv 1 \pmod 7$

$5 y_2 \equiv 1 \pmod 7$

multiply 2:

$6 y_2 \equiv 3 \pmod 7$

$\boxed{y_2 = 3 \pmod 7}$

Substitute y_1, y_2, y_3 in (1)

$2 \times 20 \times 3 + 1 \times 15 \times 3 + 3 \times 12 \times 3$

$120 + 45 + 108$

$\Rightarrow 273 \bmod 60$

$\Rightarrow 53 \pmod{60}$

$\therefore x = 60k + 53$ when $k = 0, 1, 2 \ldots$

$x \equiv 2 \pmod 3$

$x \equiv 3 \pmod 5$

$x \equiv 2 \pmod 7$ ... (1)

$a_1 m_1 y_1 + a_2 m_2 y_2 + a_3 m_3 y_3$

$2 \times 35 \times y_1 + 3 \times 21 \times y_2 + 2 \times 15 \times y_3$

$35 y_1 \equiv 1 \pmod 3$

smaller multiply with 2

$2 y_1 \equiv 1 \pmod 3$

$4 y_1 \equiv 2 \pmod 3$

$y_1 \equiv 2 \pmod 3$

$y_1 = \frac{2}{1}$

$21 y_2 \equiv 1 \pmod 5$

$1 y_2 \equiv 1 \pmod 5$

$y_2 = 1$

$15 y_3 \equiv 1 \pmod 7$

$1 y_3 \equiv 1 \pmod 7$

$y_3 = 1$

$x \equiv 2 \times 35 \times 2 + 3 \times 21 \times 1 + 2 \times 15 \times 1$

$= 140 + 63 + 30$

$= 233 \bmod 105$

$= 23$

23 is the smallest +ve integer i.e. simultaneous solution.

" " " " " that leaves a remainder of '2' when divided by '3'

'3' " " " '3'

'2' " " " '2'

(8) Solve the Congruence $4x \equiv 5 \pmod 9$

gcd $(4,9) = 1$ ∴ has a solution

$4x \equiv 5 \pmod 9$

multiply with -2

$-2.4x \equiv -2.5 \pmod 9$

apply mod 9

$-8.x \bmod 9$

$1.x \equiv 8 \pmod 9$

$x = 8$

$4x = 32 \equiv 5 \pmod 9$

$27 \pmod 9$

4×17

$68 \equiv 5 \pmod 9$

4 mod 9

$9 = 2.4 + 1$

$1 = 1.9 + (-2).4$

$= (-2)$

$1.9 \equiv 0 \pmod 9$

$-2.4 \equiv 1 \pmod 9$

$(-2)4 + 1.9 = 1$

(9) Solve $2x \equiv 7 \pmod{11}$

If 'p' is prime and 'a' is an integer not divisible by 'p', then

$$a^{p-1} \equiv 1 \pmod p$$

Furthermore, for every integer 'a' we have

$$a^p \equiv a \pmod p$$

Def ⑧

Composite integer - is not Prime
- it has factor other than '1' & itself

'1' is neither composite nor Prime

Pseudo Prime :-

It is a Probable prime, i.e, not actually prime. These are classified according to which property of primes they satisfy. Some Pseudoprimes about all probable primes, both Composite no's & actual primes

Def :- Let 'b' be a +ve integer. If 'n' is a Composite +ve integer, and $b^{n-1} \equiv 1 \pmod n$ then 'n' is called a pseudoprime to the base 'b'.

Def A Composite integer 'n' that satisfies the Congruence $b^{n-1} \equiv 1 \pmod n$ for all +ve integers 'b' with $\gcd(b,n) = 1$ is Carmichael no.

Public Key Cryptography

→ Encryption based on Congruences

Private Key cryptosystem

Ex: Cipher = (p+k) mod 26

plain = (c-k) mod 26

Public Key Cryptosystems

RSA Ronald Rivest, Adi Shamir, & Leonard Adleman

- It is based on modular exponentiation modulo the product of two large primes

RSA Encryption

In the RSA encryption method, messages are translated into sequence of integers. This can be done by translating each letter into an integer, as is done with the Caesar cipher

$C = M^e \bmod n$

$28^{13} \bmod 43$

$C^d = M \pmod{pq}$

Algorithm

So

① Each user generates a public/private key pair by

② Selecting two large primes at random - p, q

③ Computing their System modulus $N = p \times q$

$\phi(N) = (p-1)(q-1)$

④ Selecting at random the encryption key 'e'

where $1 < e < \phi(N)$, $\gcd(e, \phi(N)) = 1$

⑤ Solving following equation to find decryption key 'd'

$e.d \equiv 1 \bmod \phi(N)$ and $0 \leq d \leq N$

⑥ Publish their public encryption key

$KU = \{e, N\}$

⑦ To encrypt a message 'M' the sender

- obtain a public key reciept

$KU = \{e, N\}$

Compute $C = M^e \bmod N$ where $0 \leq M < N$

⑧ To decrypt the ciphertext 'C' the owner has

Private Key $KR = \{d, P, q\}$

$M = C^d \bmod N$

Note: $M < \text{mod } N$

$M = (M^e \bmod N)^d \bmod N$

$= M^{ed}$

$= M^{1+K(p-1)(q-1)} \pmod n$

from fermat's little theorem.

$c^d \equiv M (M^{p-1})^{k(q-1)}$

$\equiv M.1 \equiv M \pmod{p}$

& $c^d \equiv M (M^{q-1})^{k(p-1)} \equiv M.1 \equiv (M \bmod q)$

$\therefore$ $c^d = M \pmod{pq}$

(2) $T = 20$

$p = 43,\ q = 59 \quad n = 43 * 59 = 2537 \quad e = 13$

$\gcd(e, (p-1)(q-1)) = 1$

$(13, 42 \times 58) = 1$

$c =$ [illegible]

Recursive Algorithms :- (13)

An algorithm is called recursive if it solves a problem by reducing it to an instance of the same problem with smaller input

Ex: Give a recursive algorithm for computing a^n where a is a non-zero real number and 'n' is a non-negative integer.

Sol:- We can base a recursive algorithm on the recursive defination of a^n.

i.e, $a^{n+1} = a.a^n$ for $n > 0$

the initial condition $a^0 = 1$

→ To find a^n successively use the recursive condition to reduce the exponent until it becomes zero.

Recursive algorithm for computing a^n.

procedure power(a : nonzero real number, n : non-ve integer)

if $n = 0$ then power $(a, n) := 1$

else power $(a, n) := a.$ power $(a, n-1)$

Recursive Algorithm for Computing gcd(a, b)

procedure gcd(a, b : nonnegative integers with a<b)

if a=0 then gcd(a,b) := b

else gcd(a,b) := gcd(b mod a, a)

Ex: a=5, b=8

if g(5,8) = gcd(8 mod 5, 5)

= gcd(3, 5)

= gcd(5 mod 3, 3)

= gcd(2, 3)

= gcd(3 mod 2, 2)

= gcd(2 mod 1, 1)

= gcd(1, 0)

gcd(a,0) = a

gcd(1,0) = 1

13 2
2 | 13 | 6
12
1 | 2 | 1
6

2,13
0

2 | 0 | 1
0

(1, 13)

RSA (Ronald Rivest, Adi Shamir & Leonard Adleman)

→ Public key cryptography using Congruences.

RSA Encryption

1. Choose p & q.
2. Compute $n = p \times q$.
3. Compute $\phi(n) = (p-1) * (q-1)$
4. Choose 'e' such that $1 < e < \phi(n)$
   & 'e' and 'n' are coprime
5. Compute a value of 'd' such that
   $(d * e) \bmod \phi(n) = 1$
6. Public key (e,n)
7. Private key (d,n)
8. The encryption $C = M^e \bmod n$
9. The Decryption $M = C^d \bmod n$

$44+2 = 19 \times 2 + 8$

⑥ Encrypt the message STOP using RSA

$p = 43,\ q = 59 \quad n = 43 \times 59 = 2537,$ with $e = 13$

$\gcd(e, \underbrace{(p-1)(q-1)}_{\phi(n)}) = 1 \quad \gcd(13, 42 \times 58) = 1$

STOP

~~C B I T~~ (18 19) (19 15)

~~02 01 08 19~~ $\therefore \quad C = M^{13} \bmod 2537$

$(0201)^{13} \bmod 2537 = (1819)^{13} \bmod 2537 = 2081$

$(0819)^{13} \bmod 2537 = (1915)^{13} \bmod 2537 = 2182.$

$C = 2081\ 2182$

$(d \times 13 \bmod 42 \times 58) = 1.$

$d = 937$

$(2081)^{937} \bmod 2537 = (1819)$

$(2182)^{937} \bmod 2182 \quad (1915).$

$\Rightarrow$

cbit.ith1@gmail.com.

for $n = 0, 1, 2, \ldots$ where $\alpha_{i,j}$ are constants for $1 \le i \le t$

& $0 \le j \le m_i - 1$

⑦ Suppose that the characteristic polynomial for a linear homogeneous recurrence relation is $(t-2)^3 (t-3)^2 (t-4)^3$. Then the general solution is

$$a_n = (\alpha_{1,0} + \alpha_{1,1} n + \alpha_{1,2} n^2) 2^n + (\alpha_{2,0} + \alpha_{2,1} n) 3^n + (\alpha_{3,0} + \alpha_{3,1} n + \alpha_{3,2} n^2) 4^n$$

⑧ Solve the R. Relation $a_n = -3a_{n-1} - 3a_{n-2} - a_{n-3}$ with $a_0 = 1,\ a_1 = -2,\ a_2 = -1$

Ch eq $r^3 + 3r^2 + 3r + 1 = 0 \Rightarrow (r+1)^3$

$r = -1$ of multiplicity 3

$\therefore a_n = \alpha_{1,0} (-1)^n + \alpha_{1,1} n (-1)^n + \alpha_{1,2} n^2 (-1)^n$

$a_n = (1 + 3n - 2n^2)(-1)^n$

Inhomogeneous or non-homogeneous

$F(n)$	Characteristic Polynomial $C(t)$	Forms of Particular Solution a_n^p
Da^n	$C(a) \neq 0$	Aa^n
Da^n	a is a root of $C(t)$ multiplicity m	$An^m a^n$
$Dn^s a^n$	$C(a) \neq 0$	$(A_0 + A_1 n + \cdots + A_s n^s) a^n$
$Dn^s a^n$	a is a root of $C(t)$ " "	$n^m (A_0 + A_1 n + \cdots + A_s n^s) a^n$
Dn^s	$C(1) \neq 0$	$(A_0 + A_1 n + \cdots A_s n^s)$
Dn^s	1 is a root of $C(t)$ of multiplicity m	$n^m (A_0 + \cdots A_s n^s)$

Theorem ③: Let $c_1, c_2 \ldots c_k$ be real no.s Suppose that the characteristic equation

$$r^k - c_1 r^{k-1} - \cdots - c_k = 0$$

has k distinct roots $r_1, r_2 \ldots r_k$. Then a sequence $\{a_n\}$ is a solution of the recurrence relation.

$$a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k}$$

iff $a_n = \alpha_1 r_1^n + \alpha_2 r_2^n + \cdots \alpha_k r_k^n$

for $n = 0, 1, 2, \ldots$ where $\alpha_1, \alpha_2, \ldots \alpha_k$ are constants.

④ Find the solution of the recurrence relation

$$a_n = 6a_{n-1} - 11a_{n-2} + 6a_{n-3}$$

with initial conditions $a_0 = 2$, $a_1 = 5$, & $a_2 = 15$.

$$r^3 - 6r^2 + 11r - 6. \qquad r = 1, r = 2, r = 3$$

$$a_n = \alpha_1 1^n + \alpha_2 2^n + \alpha_3 3^n$$

$$\boxed{a_n = 1 - 2^n + 2 \cdot 3^n}$$

Theorem ④: Let $c_1, c_2 \ldots c_k$ be real numbers, Suppose that characteristic equation

$$r^k - c_1 r^{k-1} - \cdots - c_k = 0$$

has t distinct roots $r_1, r_2 \ldots r_t$ with multiplicities $m_1, m_2 \ldots m_t$, respectively, so that $m_i \geq 1$ for $i = 1, 2, \ldots t$ and $m_1 + m_2 + \cdots + m_t = k$. Then a sequence $\{a_n\}$ is a solution of the recurrence relation $a_n = c_1 a_{n-1} + c_2 a_{n-2} + \cdots + c_k a_{n-k}$

iff

$$a_n = (\alpha_{1,0} + \alpha_{1,1} n + \cdots + \alpha_{1,m_1-1} n^{m_1-1}) r_1^n + (\alpha_{2,0} + \alpha_{2,1} n + \cdots + \alpha_{2,m_2-1} n^{m_2-1}) r_2^n + \cdots + (\alpha_{t,0} + \alpha_{t,1} n + \cdots + \alpha_{t,m_t-1} n^{m_t-1}) r_t^n$$

⑤ Solve the recurrence $a_n - 6a_{n-1} + 8a_{n-2} = 9$ where $a_0 = 10$, and $a_1 = 25$

$$C(t): r^2 - 6r + 8 \Rightarrow (r-2)(r-4)$$

$$a_n^H = c_1 4^n + c_2 2^n$$

$$a_n^P = 9(1)^n$$

$$D(a^n) \longrightarrow Aa^n \Rightarrow 9(1)^n$$

~~$A - 6A + 8A = 9$~~

$$a_n^P = A(1)^n$$

$$A(1)^n - 6 \cdot A(1)^{n-1} + 8 \cdot A(1)^{n-2} = 9$$

$$A - 6A + 8A = 9.$$

$$3A = 9 \Rightarrow A = 3$$

$$\therefore \boxed{a_n = c_1 4^n + c_2 2^n + 3}$$

$$10 = c_1 + c_2 + 3 \Rightarrow c_1 + c_2 = 7 \quad -①$$

$$25 = 4c_1 + 2c_2 + 3 \Rightarrow 2c_1 + c_2 = 11 \quad -②$$

$$c_1 = 4, \quad c_2 = 3.$$

$$\boxed{a_n = (4)(4)^n + (3)(2)^n + 3}$$

(a) Solve $a_n - 6a_{n-1} + 8a_{n-2} = n.4^n$, where $a_0 = 8$ & $a_1 = 22$.

$a_n^p = n(A_0 + A_1 n)4^n$

$n4^n \Rightarrow \boxed{n(A_0 + A_1 n)4^n}$

$r^2 - 6r + 8 = 0$

$r^2 - 2r - 4r + 8 = 0$

$r(r-2) - 4(r-2) = 0$

$r = 2, 4$

$n(A_0 + A_1 n)4^n - 6(n-1)(A_0 + A_1(n-1))4^{n-1} + 8(n-2)(A_0 + A_1(n-2))4^{n-2} = n.4^n$

$16n(A_0 + A_1 n) - 24(n-1)(A_0 + A_1(n-1)) + 8(n-2)(A_0 + A_1(n-2)) = 16n$

$a_n^p = n(-1+n)4^n$

$p_1 n^2 + p_0 n = p_1(n-1)^2 + p_0(n-1) + n$

$p_1 n^2 + p_0 n = p_1 n^2 - 2p_1 n + p_1 + p_0 n - p_0 + n$

$2p_1 n + (p_0 - p_1) - n = 0$

$n(2p_1 - 1) + (p_0 - p_1) = 0$

$2p_1 - 1 = 0 \Rightarrow p_1 = 1/2$

$p_0 = 1/2$

$a_n^p = \frac{1}{2}n^2 + \frac{1}{2}n$

$a_n = a_n^h + a_n^p$

$= A_0 2^n + A_1 4^n + \frac{1}{2}n^2 + \frac{1}{2}n$

$a_0 = 8 \Rightarrow A_0 + A_1 = 8$

$a_1 = 22 \Rightarrow 2A_0 + 4A_1 + 1 = 22$

$2A_0 + 4A_1 = 21$

$A_0 = 11/2, \quad A_1 = 5/2$

$a_n = \frac{11}{2}2^n + \frac{5}{2}4^n + \frac{1}{2}n^2 + \frac{1}{2}n$

$= 11.2^{n-1} + 5.2^{2n-1} + \frac{1}{2}n^2 + \frac{1}{2}n$

Pigeon Hole Principle

4, 8, 10, 11, 13, 29, 33, 40, 42, 48, 57, 302, 307, 310, 311, (23) — Pairs

Generating Functions

A sequence of series of real no.'s $a_0, a_1, a_2, \ldots$ from which we can define a power series

$G(x) = a_0 + a_1 x + a_2 x^2 + \ldots$ — (1)

$\therefore G(x) = \sum_{n=0}^{\infty} a_n x^n$

$G(x)$ is generating function of the sequence $\{a_n\}$

(a) Find the G.F for the following sequences.

(a) $1, 1, 1, 1, 1, 1, 0, 0, 0, \ldots$

$G(x) = 1 + 1.x + 1.x^2 + 1.x^3 + 1.x^4 + 1.x^5 + 0.x^6 + 0.x^7 \ldots$

$= 1 + x + x^2 + x^3 + x^4 + x^5$

$\therefore G(x) = \frac{1 - x^6}{1 - x}$

(b) $1, 1, 1, \ldots$

$G(x) = 1 + x + x^2 + \ldots$

$= \frac{1}{1 - x}$

(d) Solve $a_n - 6a_{n-1} + 8a_{n-2} = n.4^n$, where $a_0 = 8$ & $a_1 = 22$.

$a_n^p = n(A_0 + A_1 n)4^n$

$n4^n \Rightarrow \boxed{n(A_0 + A_1 n)4^n}$

$r^2 - 6r + 8 = 0$

$r^2 - 2r - 4r + 8 = 0$

$r(r-2) - 4(r-2) = 0$

$r = 2, 4$

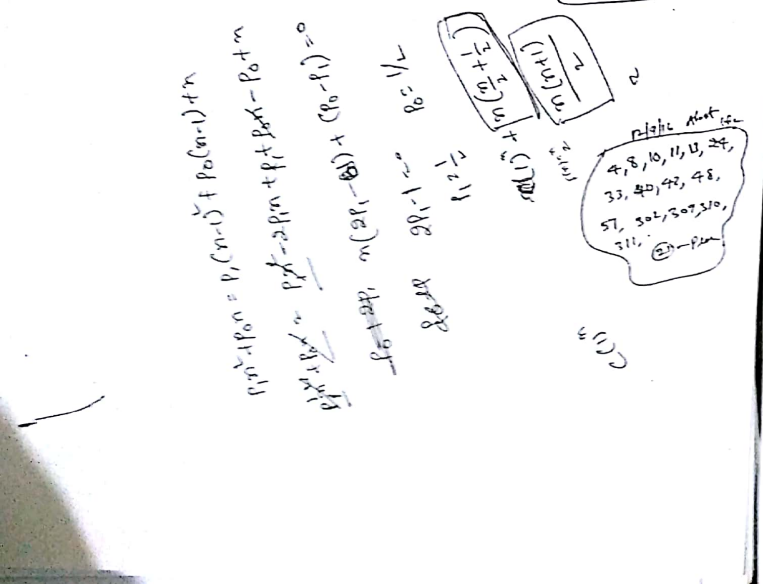
$n(A_0 + A_1 n)4^n - 6(n-1)(A_0 + A_1(n-1))4^{n-1}$

$+ 8(n-2)(A_0 + A_1(n-2))4^{n-2} = n.4^n$

$16n(A_0 + A_1 n) - 24(n-1)(A_0 + A_1(n-1))$

$+ 8(n-2)(A_0 + A_1(n-2)) = 16n$

$\boxed{a_n^p = n(-1+n)4^n}$



Generating Functions

A sequence of series of real no.'s $a_0, a_1, a_2 \ldots$ from which we can define a power series

$$G(x) = a_0 + a_1 x + a_2 x^2 + \ldots \quad (1)$$

$$\therefore G(x) = \sum_{n=0}^{\infty} a_n x^n$$

$G(x)$ is generating function of the sequence $\{a_n\}$

(a) Find the G.F for the following sequences.

(i) $1, 1, 1, 1, 1, 0, 0, 0, \ldots$

$G(x) = 1 + 1.x + 1.x^2 + 1.x^3 + 1.x^4 + 1.x^5 + 0.x^6 + 0.x^7 \ldots$

$= 1 + x + x^2 + x^3 + x^4 + x^5$

$\therefore G(x) = \frac{1 - x^6}{1 - x}$

(ii) $1, 1, 1, \ldots$

$G(x) = 1 + x + x^2 + \ldots$

$= \frac{1}{1 - x}$

Def: For any real no. u & the Int k we define the extended binomial coefficient $\binom{u}{k}$ by

$$\binom{u}{k} = \frac{u(u-1)(u-2)\cdots(u-k+1)}{k!}$$

$\binom{u}{0} = 1$ for any real no.

Problems

Thm For the integer n & r.
we have $\binom{-n}{r} = (-1)^r \binom{n+r-1}{r}$

(Q) There are 50 students in the Int Mathematical olympiad (IMO) training programme. 6 of them are to be selected to represent Hong Kong in the IMO
How many ways are there to select 6 students?

x^0 = not selected !
x^1 = selected !

$G(x) = (1+x)^{50}$.

Find $\binom{50}{6}$.

(Q) How many integer solutions to the equation $a+b+c=6$ satisfy $-1 \le a \le 2$ & $1 \le b, c \le 4$?

Sol: a contributes terms $x^{-1} + x^0 + x^1 + x^2$

b & c ~ ~ $x + x^2 + x^3 + x^4$

$$G(x) = \frac{x}{x^2}(x^{-1}+x^0+x^1+x^2)\times(1+x+x^2+x^3)\times(1+x+x^2+x^3)$$

$$= x(1+x+x^2+x^3)^3$$

$$= x\left(\frac{1-x^4}{1-x}\right)^3$$

$$= x(1-3x^4+3x^8-x^{12})(1-x)^{-3}$$

$$= (x-3x^5+3x^9-x^{13})(1-x)^{-3}$$

Here need x^5 & x in $(1-x)^{-3}$

$x\cdot\binom{-3}{5}x^5 - 3x^5\binom{-3}{1}x$ i.e. $\binom{-3}{5} - 3\binom{-3}{1}$

$\binom{-3}{5} = \frac{(-3)(-4)(-5)(-6)(-7)}{5!}$

$\binom{-3}{1} = -3$

$-3\binom{-3}{1} = 9$

$\binom{-3}{5} - 3\binom{-3}{1} = -21 + 9 = -12$

(7)

⑦ Solve the r.r. $a_n - 9a_{n-1} + 26a_{n-2} - 24a_{n-3} = 0$

for $n \geq 3$ $\quad a_0 = 0,\ a_1 = 1,\ a_2 = 10$

$$\sum_{n=3}^{\infty} a_n x^n - 9\sum_{n=3}^{\infty} a_{n-1} x^n + 26\sum_{n=3}^{\infty} a_{n-2} x^n - 24\sum_{n=3}^{\infty} a_{n-3} x^n = 0.$$

$$(A(x) - a_0 - a_1 x - a_2 x^2) - 9x\,(A(x) - a_0 - a_1 x) + 26x^2 (A(x) - a_0) - 24x^3 A(x) = 0.$$

Simplify

$$A(x)\,(1 - 9x + 26x^2 - 24x^3) = a_0 + a_1 x + a_2 x^2 - 9a_0 x - 9a_1 x^2 + 26a_0 x^2$$

Con

$$A(x) = \frac{a_0 + x(a_1 - 9a_0) + x^2(a_2 - 9a_1 + 26a_0)}{(1 - 9x + 26x^2 - 24x^3)}$$

$$\therefore \quad = \frac{C_1}{(1-2x)} + \frac{C_2}{(1-3x)} + \frac{C_3}{(1-4x)}$$

$$= C_1 \sum_{n=0}^{\infty} 2^n x^n + C_2 \sum_{n=0}^{\infty} 3^n x^n + C_3 \sum_{n=0}^{\infty} 4^n x^n.$$

$$= \sum_{n=0}^{\infty} (C_1 2^n + C_2 3^n + C_3 4^n) x^n$$

Substitute a_0, a_1, a_2

$$A(x) = \frac{0 + x(1-0) + x^2(10 - 9 + 0)}{(1-2x)(1-3x)(1-4x)}$$

⑧ Let m be a +ve integer Let $a_k = C(m,k)$ for $k = 0, 1, \ldots, m$.

what is the generating function for the sequence $a_0, a_1, \ldots, a_m$

$$G(x) = C(m,0) + C(m,1)x + C(m,2)x^2 + \cdots + C(m,m)x^m$$

$$G(x) = (1+x)^m$$

c ~~$(1+x)^{-1} = \binom{-1}{0} 1 + \binom{-1}{1} 1^{n-1} x + \binom{-1}{2} 1^{n-2} x^2 + \cdots$~~

Bcz series

$$\sum_{k=0}^{n-1} (ar^k) = a\left(\frac{1-r^n}{1-r}\right)$$

$$\sum_{k=0}^{\infty} (ar^k) = a\left(\frac{1}{1-r}\right)$$

$r^{\infty} = 0$

$1, 1, 1 \ldots$

$$f(x) = \frac{1}{(1-x)} = 1 + x + x^2 + \cdots = \sum$$

$$\frac{1}{(1-ax)} = 1 + ax + a^2x^2 + \cdots$$

$1, a, a^2, a^3 \ldots$

$f(n) = c_1 n^{\log_b a} + c_2$,

$a^k = a^{\log_b n} = n^{\log_b a}$

$\log_a a^k = \log_a a^{\log_b n}$

$k = \log_b n \Rightarrow$

Generating functions

(a) $f(x) = 1/(1-x)$ is the function of sequence $1, 1, \ldots$

$1/(1-x) = 1 + x + x^2 + \ldots$

Theorem: Let $f(x) = \sum_{k=0}^{\infty} a_k x^k$ and $g(x) = \sum_{k=0}^{\infty} b_k x^k$.

Then $f(x) + g(x) = \sum_{k=0}^{\infty} (a_k + b_k) x^k$ +

$f(x) \cdot g(x) = \sum_{k=0}^{\infty} \left(\sum_{j=0}^{k} a_j b_{k-j} \right) x^k$

(a) Let $f(x) = \frac{1}{(1-x)^2}$, find the co-efficients $a_0, a_1, \ldots$ in the expansion $f(x) = \sum_{k=0}^{\infty} a_k x^k$

Sol $\frac{1}{(1-x)} = 1 + x + x^2 + x^3 + \ldots = \sum_{k=0}^{\infty} x^k$

$\frac{1}{(1-x)^2} = \sum_{k=0}^{\infty} (\quad$

$1, 2, 4, 6, 8, \ldots$

$f(x) = \frac{1}{(1-x)}$, $g(x) = \frac{1}{(1-x)}$

$f(x) \cdot g(x) = \sum_{k=0}^{\infty} \left(\sum_{j=0}^{k} 1 \right) x^k$

Def Let 'u' be the real number & k a non-negative integer. Then the extended binomial co-efficient $\binom{u}{k}$ is defined by

$$\binom{u}{k} = \begin{cases} u(u-1)\ldots(u-k+1)/k! & \text{if } k > 0 \\ 1 & \text{if } k = 0 \end{cases}$$

(a) Find the value of Gelen $\binom{-2}{3}$ $\binom{1/2}{3}$

$k - k + 1 = -2$

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

$= \frac{-4}{2}$

$u = \frac{1}{2}$ $\quad k = 3$

$\frac{1}{2} - 3 + 1$

$$\binom{\frac{1}{2}}{3} = \frac{\left(\frac{1}{2}\right)\left(\frac{1}{2}-1\right)\left(\frac{1}{2}-2\right)}{3!}$$

$$= \frac{1}{16} \qquad 2^{-\frac{1}{1}}$$

(a) When the top param is -ve integer.

$$\binom{-n}{r} = \frac{(-n)(-n-1)\cdots(-n-r+1)}{r!}$$ (of Extended Binomial Co-eff)

$$= \frac{(-1)^r\, n(n+1)\cdots(n+r-1)}{r!}$$ out -1 in nn

$$= \frac{(-1)^r (n+r-1)(n+r-2)\cdots n}{r!}$$ Commutative

$$= \frac{(-1)^r (n+r-1)!}{r!\,(n-1)!} \qquad (n-1)!$$

$$= (-1)^r \binom{n+r-1}{r}$$

$$= (-1)^r\, C(n+r-1, r)$$

Extended Binomial ①

Let x be a real no. with $|x| < 1$ &

let u be real no.

$$\therefore \boxed{(1+x)^u = \sum_{k=0}^{\infty} \binom{u}{k} x^k}$$

(b) Find the generating function for $(1+x)^{-n}$ & $(1-x)^{-n}$ where n is a +ve integer using the extended Binomial Theorem.

$$(1+x)^{-n} = \sum_{k=0}^{\infty} \binom{-n}{k} x^k$$

$$= \sum_{k=0}^{\infty} (-1)^k\, C(n+k-1, k)\, x^k$$

Replacing x by $-x$

$$(1-x)^{-n} = \sum_{k=0}^{\infty} C(n+k-1, k)\, x^k.$$

	$G(x)$	a_k
①	$(1+x)^n = \sum_{k=0}^{n} C(n,k)\, x^k$ $= 1 + C(n,1)x + C(n,2)x^2 + \cdots + x^n$	$C(n,k)$
②	$(1+ax)^n = \sum_{k=0}^{n} C(n,k)\, a^k x^k$ $= 1 + C(n,1)ax + C(n,2)a^2x^2 + \cdots + a^n x^n$	$C(n,k)\, a^k$
③	$(1+x^r)^n = \sum_{k=0}^{n} C(n,k)\, x^{rk}$ $= 1 + C(n,1)x^r + C(n,2)x^{2r} + \cdots + x^{rn}$	1 if $r \mid k$; 0 otherwise
④	$\frac{1-x^{n+1}}{1-x} = \sum_{k=0}^{n} x^k = 1 + x + x^2 + \cdots + x^n$	1 if $k \le n$; 0 otherwise
⑤	$\frac{1}{1-x} = \sum_{k=0}^{\infty} x^k = 1 + x + x^2 + \cdots$	1
⑥	$\frac{1}{1-ax} = \sum_{k=0}^{\infty} a^k x^k = 1 + ax + a^2x^2 + \cdots$	a^k
⑦	$\frac{1}{1-x^r} = \sum_{k=0}^{\infty} x^{rk} = 1 + x^r + x^{2r} + \cdots$	1 if $r \mid k$; 0 otherwise.
⑧	$\frac{1}{(1-x)^2} = \sum_{k=0}^{\infty} (k+1)x^k = 1 + 2x + 3x^2 + \cdots$	$k+1$
⑨	$\frac{1}{(1-x)^n} = \sum_{k=0}^{\infty} C(n+k-1,k)\, x^k$ $= 1 + C(n,1)x + C(n+1,2)x^2 + \cdots$	$C(n+k-1,k)$ $= C(n+k-1,n-1)$
⑩	$\frac{1}{(1+x)^n} = \sum_{k=0}^{\infty} C(n+k-1,k)(-1)^k x^k$ $= 1 - C(n,1)x + C(n+1,2)x^2 - \cdots$	$(-1)^k C(n+k-1,k)$ $= (-1)^k C(n+k-1,n-1)$
⑪	$\frac{1}{(1-ax)^n} = \sum_{k=0}^{\infty} C(n+k-1,k)\, a^k x^k$ $= 1 + C(n,1)ax + C(n+1,2)a^2x^2 + \cdots$	$C(n+k-1,k)\, a^k$ $= C(n+k-1,n-1)\, a^k$

	$G(x)$	a_k
⑫	$e^x = \sum_{k=0}^{\infty} \frac{x^k}{k!} = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots$	$\frac{1}{k!}$
⑬	$\ln(1+x) = \sum_{k=0}^{\infty} \frac{(-1)^{k+1}}{k} x^k = x - \frac{x^2}{2} + \frac{x^3}{3} - \frac{x^4}{4} + \cdots$	$(-1)^{k+1}/k$

Counting Problems and Generating Functions

① Find the no. of solutions of

$e_1 + e_2 + e_3 = 17$

where e_1, e_2, e_3 are non-negative integers with ~~$2 \le e_1 \le 5$~~, $3 \le e_2 \le 6$ & $4 \le e_3 \le 7$

∴ The no of solutions with the indicating constraints

$(x^2+x^3+x^4+x^5)(x^3+x^4+x^5+x^6)(x^4+x^5+x^6+x^7)$

$x^2(1+x+x^2+x^3)\cdot x^3(1+x+x^2+x^3)\cdot x^4(1+x+x^2+x^3)$

$x^9(1+x+x^2+x^3)^3$

$x^9\frac{(1-x^4)^3}{(1-x)^3} \Rightarrow$?

$x^9(1-3x^4+3x^8-x^{12})$

$= 3x^{17}$

$x^9(1+x)(1+x^2)^3$

$(1-x)^3$ $= 0$

$x^9(1-3x^4+3x^8-x^{12}) = 0.$

$(3)x^{17}$

(5) In how many different ways can eight identical cookies be distributed among three distinct children if each child receives at least two cookies & no more than 4 cookies?

$(x^2+x^3+x^4)^3 \Rightarrow x^6(1+x+x^2)^3$ $\quad x^3 = ?$

$\Rightarrow x^6\left(\frac{1-x^3}{1-x}\right)^3$

$\Rightarrow x^6\left((1-x^3)^3 \times (1+3x+\frac{3\cdot4}{2}x^2+\cdots)\right)$

$\Rightarrow 6x^6$

Solve Hypothesis: Let $G(x) = \sum_{n=0}^{\infty} a_n x^n$

$\sum_{n=0}^{\infty} a_n x^n = G(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{k-1}x^{k-1} + \cdots$

$\sum_{n=0}^{\infty} a_{n-1} x^n = xG(x) = a_0 x + a_1 x^2 + a_2 x^3 + \cdots + a_{k-1}x^k + \cdots$

$\sum_{n=0}^{\infty} a_{n-2} x^n = x^2 G(x) = a_0 x^2 + a_1 x^3 + a_2 x^4 + \cdots + a_{k-2}x^k + \cdots$

$\sum_{n=k}^{\infty} a_n x^n = G(x) - a_0 - a_1 x - \cdots - a_{k-1}x^{k-1}$

$\sum_{n=k}^{\infty} a_{n-1} x^n = x\left(G(x) - a_0 - a_1 x - \cdots - a_{k-2}x^{k-2}\right)$

$\sum_{n=k}^{\infty} a_{n-2} x^n = x^2\left(A(x) - a_0 - a_1 x - \cdots - a_{k-3}x^{k-3}\right)$

$x^3\left(\quad\right)$ $\quad n=k$

$\sum_{n=k}^{\infty} a_{n-k} x^n = x^k\left(A(x)\right)$

Solve the recurrence rel

Steps:

① Let $G(x) = \sum_{n=0}^{\infty} a_n x^n$

② Multiply with x^n & sum from k to ∞.

③ Replace each term with expression

④ Solve $a_k = 3a_{k-1}$ for $k = 1, 2, 3, \cdots$ $\quad a_0 = 2$.

$G(x) = \sum_{k=0}^{\infty} a_k x^k$

$xG(x) = \sum_{k=0}^{\infty} a_k x^{k+1} \Rightarrow \sum_{k=1}^{\infty} a_{k-1} x^k$

$G(x) - 3xG(x) = \sum_{k=0}^{\infty} a_k x^k - 3\sum_{k=1}^{\infty} a_{k-1} x^k$

$= a_0 + \sum_{k=1}^{\infty} (a_k - 3a_{k-1}) x^k$

2

$\Rightarrow G(x) = \frac{2}{(1-3x)}$

Q. $a_n = 3a_{n-1}$ $a_0 = 2$ (1)

(1) multiply with x^n & n = Sum 1 to ∞

$$\sum_{n=1}^{\infty} a_n x^n - 3\sum_{n=1}^{\infty} a_{n-1} x^n = 0$$

$$A(x) - 3x[A(x) - a_0] = 0$$

$$A(x)(1-3x) = a_0 \Rightarrow$$

$$A(x) = \frac{2}{(1-3x)}$$

$$A(x) = 2\sum_{x=0}^{\infty} 3^n x^n$$

$$\sum_{n=0}^{\infty} a_n x^n = 2\sum_{x=0}^{\infty} 3^n x^n$$

$$\boxed{a_n = 2.3^n}$$

(a) $a_n = 8a_{n-1} + 10^{n-1}$ $\quad a_1 = 9, \quad a_0 = 1$

Multiply with $\sum_{n=1}^{\infty} x^n$ & sum 1 to ∞

$$\sum_{n=1}^{\infty} a_n x^n = 8\sum_{n=1}^{\infty} a_{n-1} x^n + \sum_{n=1}^{\infty} 10^{n-1} x^n$$

$$A(x) - a_0 = 8x(A(x) - a_0) + x \sum_{n=1}^{\infty} 10^{n-1} x^{n-1}$$

$$= 8x(A(x) - a_0) + x \sum_{n=0}^{\infty} 10^n x^n$$

$$= 8x(A(x) - a_0) + \frac{x}{1-10x}$$

$$= \frac{8x(A(x) - a_0) + x}{(1-10x)}$$

$$= 8x \sum_{n=1}^{\infty} a_{n-1} x^{n-1} + x \sum_{n=1}^{\infty} 10^{n-1} x^{n-1}$$

$$= 8x \sum_{n=0}^{\infty} a_n x^n + x \sum_{n=0}^{\infty} 10^n x^n$$

$$G(x) - 1 = 8x G(x) + \frac{x}{(1-10x)}$$

$$G(x) - 1 - 8x G(x) = \frac{x}{(1-10x)}$$