· permutations & combinations

Combinatorics.

Basic counting principles :-

1. rule of product :- if one experiment has m possible outcomes and another experiment has 'n' possible outcomes. Then there are m×n possible outcomes when both of these experiment takes place.

Eg :-

How many different bit strings are there of length (9)

since each bit is either 0 or 1 each bit can be choose in two ways there fore by the product rule the number of different bit strings of length of 9 is $2^9 = 512$

2. Rule of sum :-

if one experiment has m possible outcomes and another experiment has n' possible out comes then there are m+n possible outcomes when exactly one of these experiment takes place.

Ex :-

A student can be choose a computer project from one of five atleast the five last contain 15, 12, 9, 10 & 20 projects respectively. How many possible are there to choose them?

The student can be choose a computer project from the 1st list is 15 and from 2nd list is 12, 3rd list 9 and 4th list 10 & fifth list is 20

$\therefore$ the no.of possible projects $= 15+12+9+10+20$
$= 66$

permutations

An ordered arrangement of objects from a set of different objects is called a permutation.

that is the number of 'r' permutation of a set with 'n' different elements is

$$^{n}P_{r} \text{ (or) } P(n,r) = \frac{n!}{(n-r)!}$$

1. find the number of five permutations of a set with Nine elements?

$$^{n}P_{r} = \frac{n!}{(n-r)!} \quad \text{Here } n=9, r=5$$

$$\frac{9!}{(9-5)!} = \frac{9\times8\times7\times6\times5\times\cancel{4\times3\times2\times1}}{\cancel{4\times3\times2\times1}}$$

$$= 15120$$

2. list all the permutations of $\{a,b,c\}$

$$^{n}P_{r} = \frac{n!}{(n-r)!} \quad \text{Here } n=3 \; r=3$$

$$= \frac{3!}{(3-3)!} = \frac{3!}{0!}$$

$$= 3\times2$$

$$= 6$$

$$\therefore (0! = 1)$$

3. How Many permutations are $\{a, b, c, d, e, f, g\}$ End with a ?

$\boxed{}\ \boxed{}\ \boxed{}\ \boxed{}\ \boxed{}\ \boxed{}\ \boxed{a}$

6 5 4 3 2 1

$6! = 720$

4. suppose repetations are not permitted answer the following questions

1. How many three digit numbers from the six digits 2 3 5 6 7 and 9 ?

2. How many of these numbers are less than 400 ?

3. How many of these are Even?

1)

$\overset{6}{\boxed{}}\ \overset{5}{\boxed{}}\ \overset{4}{\boxed{}}$

$6 \times 5 \times 4 = 120$

2)

$\overset{2}{\boxed{}}\ \overset{5}{\boxed{}}\ \overset{4}{\boxed{}}$

<400 200 or 3

$2 \times 5 \times 4 = 40$

3)

$\overset{4}{\boxed{}}\ \overset{5}{\boxed{}}\ \overset{2}{\boxed{}}$

$4 \times 5 \times 2 = 40$

* Find the no. of 3 digits even no. with no repeated digits

sol :-

7	9	5
$\square$	$\square$	$\square$

0 1 2 3 4 5 6 7 8

$7 \times 9 \times 5 = 63 \times 5$

$\Rightarrow 315$

* Find n, if (i) $P(n,2) = 72$

(ii) $P(n,4) = 42\,P(n,2)$

(iii) $2P(n,P) + 50 = P(2n,2)$

(i) given $P(n,2) = 72$,

By defination $^nP_r = \frac{n!}{(n-r)!}$

We know that,

$$P(n,r) = {}^nP_r = \frac{n!}{(n-r)!}$$

$\therefore$ given, $P(n,2) = 72$

$$P(n,r) = \frac{n!}{(n-r)!} = 72$$

$$P(n,2) \Rightarrow \frac{n!}{(n-2)!} = 72.$$

$$\therefore \frac{\cancel{1\times2\times3\times4\times\cdots(n-2)}(n-1)\times n}{\cancel{1\times2\times3\times4\times\cdots(n-2)}} = 72$$

$\therefore (n-1)n = 72$

$\therefore n^2 - n - 72 = 0$

Nowe we find factors,

$n^2 - 9n + 8n - 72$

$n(n-9) + 8(n-9)$

$(n-9)(n+8)$

$n = 9, -8 \Rightarrow$ (We can consider only +ve value)

Here, $n = 9$

(ii) given $P(n,4) = 42\, P(n,2)$

By the defination $^nP_r = \frac{n!}{(n-r)!}$

We know that,

$$P(n,r) = {}^nP_r = \frac{n!}{(n-r)!}$$

$\therefore$ given, $P(n,4) = 42$

$$P(n,r) = \frac{n!}{(n-r)!} = 42\, P(n,2)$$

$$P(n,4) = \frac{n!}{(n-4)!} = 42\, P(n,2)$$

$$P(n,4) = \frac{n!}{(n-4)!} = 42\, \frac{n!}{(n-2)!}$$

$$\frac{\cancel{1\times2\times3\times4\times\cdots}(n-4)(n-3)(n-2)(n-1)n}{\cancel{1\times2\times3\times\cdots(n-4)}} = 42\,\frac{\cancel{1\times2\times3\times(n-2)}(n-1)n}{\cancel{1\times2\times3\times\cdots(n-2)}}$$

$$(n-3)(n-2)\cancel{(n-1)n} = 42\cancel{(n-1)n}$$

$$(n-3)(n-2) = 42$$

$$n^2 - 2n - 3n + 6 = 42$$

$$n^2 - 5n + 6 - 42 = 0$$

$$n^2 - 5n - 36 = 0$$

$$n^2 - 9n + 4n - 36 = 0$$

$$n(n-9) + 4(n-9) = 0$$

$$(n-9)(n+4) = 0$$

$$n = 9, -4$$

$\boxed{\therefore n = 9}$, (negative values does not consider)

(iii) given, $2P(n,2) + 50 = P(2n,2)$

By defination of,

$$\Rightarrow 2P\frac{n!}{(n-2!)} + 50 = \frac{2n!}{(2n-2)!}$$

$$\Rightarrow 2 \cdot \frac{\cancel{1\times2\times3\times\cdots(n-2)}(n-1)n}{\cancel{1\times2\times3\cdots\cdots(n-2)}} + 50 = \frac{\cancel{1\times2\times3\times\cdots(2n-2)}(2n-1)(2n)}{\cancel{1\times2\times3\times\cdots(2n-2)}}$$

$$\Rightarrow 2(n-1)n + 50 = (2n-1)(2n)$$

$$\Rightarrow \cancel{2n^2} - \cancel{2n} + 50 = 4\cancel{n^2} - \cancel{2n}$$

$$\Rightarrow \cancel{50}^{25} = \cancel{2}n^2$$

$25 = n^2$

$\boxed{\therefore n = 5}$

* **Permutation with repetition :-**

→ The Number of 'r' permutations of a set of small n objects with repetetion allowed is (n^r)

→ if there are n_1 objects of type-1 n_2 objects of type 2 ------ n_k objects of type(k) Then The no.of different permutations of (n) objects is $\frac{n!}{n_1! \cdot n_2! --- n_k!}$

* How many different strings can be made from the letters of the word "SUCCESS" using the all letters.

given word "success"

total no.of letters $n = 7$

The word success contains

$3's$, $2'cs$, $1'e$, $1'u$

$\therefore$ total no.of arrangement $= \frac{7!}{3!2!1!1!}$

$$= \frac{7 \times 6 \times 5 \times \overset{2}{\cancel{4}} \times \cancel{3 \times 2 \times 1}}{\cancel{3 \times 2 \times 1} \times \cancel{2} \times 1 \times 1 \times 1}$$

$= 420$

→ "ABRACADABRA"

→ "Engineering"

→ "MATHEMATICS"

sol: given word is 'ABRACADABRA'

total no.of letters, $n = 11$

The word ABRACADABRA contains

5 A's,

2 B's

2 R's

1 C

1 D

$$\text{total no.of arrangement} = \frac{11!}{5!\,2!\,2!\,1!\,1!}$$

$$\Rightarrow \frac{11 \times 10 \times 9 \times \overset{4}{\cancel{8}} \times 7 \times \overset{3}{\cancel{6}} \times \cancel{5 \times 4 \times 3 \times 2 \times 1}}{\cancel{5 \times 4 \times 3 \times 2 \times 1} \times \cancel{2} \times 1 \times \cancel{2} \times 1 \times 1 \times 1}$$

$\Rightarrow 83160$

combinations :- The no.of "r" combinations of a set with 'n' elements where 'n' is a non-negative integer and 'r' is an integer with $0 \le r \le n$ is,

$$nC_r \text{ (or) } C(n,r) = \frac{n!}{(n-r)!\,r!}$$

A club has 25 members. How many ways are there to choose 4 members of the club to serve an executive commitee? choose selection.

Sol :- Total no. of club members, $n = 25$

The number of committe members $= 4$

$\therefore r = 4$

Total number of ways are selecting 4 member of commitee with 25 Members is,

$$25C_4 = \frac{25!}{(25-4)!\,4!} = \frac{(25)!}{(21)!\,4!}$$

$$\Rightarrow \frac{25 \times \cancel{24}^{10} \times 23 \times 22 \times \cancel{21 \times 20 \times 19 \times 18 \times 17 \times 16 \times 15 \times 14 \cdots \times 1}}{\cancel{21 \times \cdots \times 1} \times \cancel{4 \times 3 \times 2 \times 2 \times 1}}$$

$\Rightarrow 12650$

How many bit strings of length "8" contains

(i) exactly 5 1's

(ii) And equal number of 0's and 1's

(iii) Atleast 4 1's

(iv) Atleast 3 1's and Atleast 3 0's.

1'	0'
$8C_3$	$8C_5$
$8C_4$	$8C_4$
$8C_5$	$8C_3$

Sol :- (i) $8C_5$

(ii) $8C_4$ and $8C_4$

(iii) $8C_4 + 8C_5 + 8C_6 + 8C_7 + 8C_8$

(iv) $8C_3 + 8C_4 + 8C_5$

→ suppose a department consists of 8 men and 9 women in how many ways can we select a comittee of

(i) 3 men and 4 women

(ii) 4 persons that has atleast one women

(iii) 4 persons that has atmost one man

(iv) 4 persons that has both sex

(v) 4 persons such that two specific members are not included combination with repeatetion:-

if the repetetion of elements is allow then the no. of 'r' combinations form as a set of elements is $^{n+r-1}C_r$ (or) $c(n+r-1, r)$

problem:

There are three boxes of identical Red, blue and white balls. where each ~~ball~~ box contains atleast 10 balls. How many ways are there to select 10 balls if

(i) There is no restriction
(ii) Atleast one white ball must be selected
(iii) Atleast one red ball, Atleast two blue balls and Atleast three white balls must be selected
(iv) ~~exactly one red ball must be selected~~
(iv) exactly one red ball must be selected
(v) exactly one red ball and atleast one blue ball must be selected
(vi) atmost one white ball is selected
(vii) twice as many red ~~balls~~ balls as white balls must be selected

(i) There are three kinds of balls. and we have to select 10 balls. since no restrictions, therefore repetetion is allowed. Hence the no. of ways are selecting 10 balls is

$^{n+r-1}C_r$,

Here, $n=3$
$r=10$,
substitue n, r values above,

$\Rightarrow {}^{n+r-1}C_r$

$\Rightarrow {}^{3+10-1}C_{10}$

$\Rightarrow {}^{12}C_{10}$

$\Rightarrow 66$

(ii) We select one white ball and keep it seperately. Then we have to select Nine(9) balls from the 3 kinds of balls. and then include the first white ball in this selection. hence. the required no.of ways of selecting 10 balls. is,

$n=3$

$r=9$

$^{n+r-1}C_r$

Here, $n=3$
$r=9$

substitute above formula, in n, r, values, $\Rightarrow {}^{3+9-1}C_9$

$\Rightarrow {}^{11}C_9$

$\Rightarrow 55$

(iii) if we select one red ball, two blue balls, 3 white balls keep it seperately, Then we select 4 balls from the three kinds of balls and include the 1st 6 balls in each selection.

Hence the required no. of ways of selecting 10 ball's is

$$^{n+r-1}C_r$$

Here,

$n=3$

$r=4$

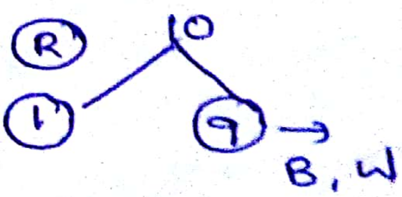
substitue above formula for the n, r values

$\Rightarrow {}^{3+4-1}C_r$

$\Rightarrow {}^{6}C_4$

$\Rightarrow 15$

(iv) if we select exactly one red ball and keep it seperately, then we select '9' balls from the two kind of balls then include one red ball in each selection.



Hence the required no. of ways of selecting 10 ball's is.

$n+r-1C_r$

$n=2$

$r=9$

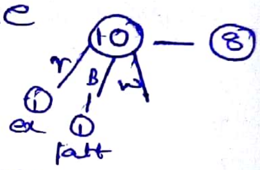
$\Rightarrow 2+9-1C_9$

$\Rightarrow 11-1C_9$

$\Rightarrow 10C_9$

$\Rightarrow 10$

(v) We select one red and one blue ball and keep it sepereately then, we select 8 balls from the 2 kinds of balls and include first two balls in each ~~suggestion~~ selection



$\therefore$ The required no. of ways of selection from 10 balls is;

$n=2$

$r=8$

$\Rightarrow n+r-1C_r$

$\Rightarrow 2+8-1C_r$

$\Rightarrow 9C_8$

$$\Rightarrow \frac{9\times\cancel{8\times7\times6\times5\times4\times3\times2\times1}}{(9-8)!\ \cancel{8\times7\times6\times5\times4\times3\times2\times1}}$$

$\Rightarrow 9$

(vi)

$$\begin{array}{cccc} & W & W & \\ & 0 & 1 & \\ 10 & B & R & W \end{array}$$

$n=2$ $\qquad$ $n=2$

$2+10-1C_r$ $r=10$ $\qquad$ $r=9$

$\Rightarrow 11C10$ $\qquad$ $\Rightarrow 2+9-1C_9$

$\Rightarrow 10C9.$

$\Rightarrow 11C_{10}+10C9$

We ~~must~~ need atmost one white ball ~~H~~ence the selection must not contain a white ball (or) contain a white ball.

the no.of ways of selection of 10's balls is

contain White ball is,

$n+r-1C_r$

$n=2$

$r=9$

$2+9-1C9$

$11-1C9$

$10C9$

not contain White ball is,

$n+r-1C_r$

$n=2$

$r=10$

$n+r-1C_r$

$2+10-1C_{10}$

$12-1C_{10}$

$11C_{10}$

Now the sum will be

$\Rightarrow 11C_{10} + 10C_9 \Rightarrow 21$

$$\Rightarrow \frac{11\times\cancel{10\times9\times8\times7\times6\times5\times4\times3\times2\times1}}{(11-10)!\ \cancel{10\times9\times8\times7\times6\times5\times4\times3}} + \frac{\cancel{10\times9\times8\times7\times6\times5\times4\times3\times2}}{(10-9)!\ \cancel{9\times8\times7\times6\times5}}$$

$\Rightarrow 11+10$

$\Rightarrow 21$

(viii) The selection must contain, 0 Red & 0 white, 2 red & 1 white balls, 4 red & 2 white balls, 6 red & 3 white balls,

The no. of ways of selection

R	W		B	
0	0	=0	10	⇒ 9
2	1	=3	7	⇒ 9
4	2	=6	4	⇒ 9
6	3	=9	1	⇒ 9

1st condition :- $n+r-1$

$n=1$

$r=10$

$1+10-1C_r \Rightarrow 10C_{10}$

$2^{nd} \Rightarrow n+r-1C_r$

$n=1$

$r=7$

$1+7-1C_7$

$7C_7$

$3^{rd} \Rightarrow n+r-1C_r$

$n=1$

$r=4$

$1+4-1C_4 \Rightarrow 4C_4$

$4^{th} \Rightarrow n+r-1C_r$

$1+1-1C_1$

$n=1$

$r=1$

$nC_i\, x^{n-i} y^i$

$\Rightarrow 1C_1$

$nC_i\, x^{n-i} y^i$

$\Rightarrow 10C_{10} + 7C_7 + 4C_4 + 1C_1$

$\Rightarrow 1+1+1+1$

$\Rightarrow 4$

Binomial theorem :-

let x & y be any two variables and 'n' be a non-negative integer. Then,

$$\boxed{(x+y)^n = \sum_{i=0}^{n} nC_i\, x^{n-i} y^i}$$

Problem

(1) find the coefficent of x^5y^8 in $(x+y)^{13}$.

Given x^5y^8 in $(x+y)^{13}$

By defination of Binomial theorem.

$$(x+y)^n = \sum_{r=0}^{n} nC_r\, x^{n-r} y^r$$

$$(x+y)^n = nC_r\, x^{n-r} y^r$$

$$\Rightarrow n-r=5 \quad , \quad r=8$$

$$13-r=5$$

$$13-8=5$$

$$5=5$$

$$1$$

$13C_8\, x^5 y^8$,

$$13C8 \Rightarrow \frac{13\times12\times11\times10\times9\times\cancel{8\times7\times6\times5\times4\times3\times2\times1}}{5!\quad \cancel{8\times7\times6\times5\times4\times3\times2\times1}}$$

$$\left\{\Rightarrow \frac{13\times12\times\cancel{11}\times\cancel{10}\times9\times\cancel{8}\times9}{\cancel{5}\times\cancel{2}\times\cancel{4}\times\cancel{3}\times\cancel{2}\times1}\right\} \text{wrong}$$

$$\Rightarrow \frac{13\times\cancel{12}\times11\times\cancel{10}\times9}{\cancel{5}\times\cancel{4}\times\cancel{3}\times\cancel{2}\times1}$$

$$\Rightarrow 1287\, x^5y^8$$

$x^{101}\ y^{99}\ (2x-3y)^{200}$

Given $x^{101}, y^{99}\ (2x-3y)^{200}$

By defination of Binomial theorem

$$(x+y)^i = \sum_{i=0}^{n} nc_i\, x^{n-i}\, y^i$$

$$(x+y)^i = nc_i\, x^{n-i}\, y^i$$

$$\Rightarrow 200c_{99}\ (2x)^{101}\ (-3y)^{99}$$

$$\Rightarrow 200c_{99}\ 2^{101}\ (+3)^{99}\ x^{101}\ (+y)^{99}$$

③ if n is a non negative integer. show that $\sum_{i=0}^{n} nc_i = 2^n$.

Sol :- By $(x+y)^n = \sum_{i=0}^{n} nc_i\, x^{n-i}\, y^i$

put $x=1$ & $y=1$

$$(2)^n = \sum_{i=0}^{n} nc_i\, (1)^{n-i}\, (1)^i$$

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

④ if n is a non negative integer show that,

$$\sum_{i=0}^{n} (-1)^i\, nc_i = 0$$

Sol : By $(x+y)^n = \sum_{i=0}^{n} nc_i\, x^{n-i}\, y^i$

put $x=1$ & $y=-1$

$$0 = \sum_{i=0}^{n} nc_i \, (1)^{n-i} (-1)^i$$

$$0 = \sum_{i=0}^{n} nc_i \, (-1)^i$$

⑤ if n is a non-negative integer, show that, $\sum_{i=0}^{n} nc_i \, 2^i = 3^n$.

sol :- By $(x+y)^n = \sum_{i=0}^{n} nc_i \, x^{n-i} y^i$

put $x=1$ $y=2$

$$(1+2)^n = \sum_{i=0}^{n} nc_i \, (1)^{n-i} (2)^i$$

$$(3)^n = \sum_{i=0}^{n} nc_i \, 2^i$$

$$\sum_{i=0}^{n} nc_i (2)^i = 3^n$$

Multinomial coefficents : given non-negative integers, $k_1, k_2, k_3 \ldots k_m$ and $n = k_1 + k_2 + \ldots + k_m$
The multinomial coefficents is $\binom{n}{k_1!\, k_2!\, k_3! \ldots k_m!}$

i.e's $\binom{n}{k_1!\, k_2!\, k_3! \ldots k_m!} = \dfrac{n!}{k_1!\, k_2!\, k_3! \ldots k_m!}$

find the coefficent of $x^3 y^3 z^2 (2x - 5y + 5z)^8$

Sol :- given, $x^3 y^3 z^2 (2x - 5y + 5z)^8$

Here, $n = 8$
$k_1 = 3$
$k_2 = 3$
$k_3 = 2$

We know that, $\dfrac{n!}{k_1!\, k_2!\, k_3! \ldots k_m!}$

$\Rightarrow \dfrac{8!}{3!\, 3!\, 2!} (2x)^3 (-5y)^3 (5z)^2$

$\Rightarrow \dfrac{8!}{3!\, 3!\, 2!} 2^3 x^3 (-5)^3 y^3 5^2 z^2$

$\Rightarrow \dfrac{8!}{3!\, 3!\, 2!} 2^3 (-5)^3 (5)^2 \cdot x^3 y^3 z^2$

$\Rightarrow \dfrac{8 \times 7 \times 6 \times 5 \times 4 \times 3 \times 2 \times 1}{3 \times 2 \times 1 \times 3 \times 2 \times 1 \times 2 \times 1}$

find the coefficent of $u^2 w^3 x^4 y^2$ in the expansion $(u + v + 2w + x + 3y + z)^{11}$.

Sol :- Given $u^2 w^3 x^4 y^2 (u + v + 2w + x + 3y + z)^{11}$

Here, $n = 11$
$k_1 = 2$
$k_2 = 3$
$k_3 = 4$, $k_4 = 2$.

We know that $\dfrac{n!}{k_1!\,k_2!\,k_3!\,\cdots k_m!}$

$$\Rightarrow \frac{11!}{2!\,3!\,4!\,2!} (u)^2 (v)^0 (2w)^3 (x)^4 (3y)^2 (z)^0$$

$$\Rightarrow \frac{11!}{2!\,3!\,4!\,2!} u^2\, 2^3 w^3 x^4\, 3^2 y^2$$

$$\Rightarrow \frac{11!}{2!\,3!\,4!\,2!} (u^2 w^3 x^4 y^2)\, 2^3\, 3^2$$

Multinomial theorem :-

→ let $a_1, a_2 \cdots a_m \in R$ & $n \in Z$ with $n \geq 1$ Then

$$(a_1 + a_2 + a_3 + \cdots + a_m)^n = \sum_{\substack{0 \leq k_1, k_2 \cdots k_m \leq n \\ k_1 + k_2 + \cdots + k_m = n}} \binom{n}{k_1, k_2 \cdots k_m} a_1^{k_1} a_2^{k_2} \cdots a_m^{k_m}$$

→ Here the sum is indexed over all ordered 'm' integers $k_1, k_2 \cdots k_m$ $\forall$ $0 \leq k_1, k_2 \cdots k_m \leq n$ and

$$k_1 + k_2 + k_3 + \cdots k_n = n$$

→ let us $(a_1 + a_2 + \cdots + a_m)(a_1 + a_2 + \cdots + a_m) \cdots (a_1 + a_2 + \cdots$ n times. Here choosing the value a_{i1} from the sumation in the first factor a_{i2}. from the sumation of the second factor

$a_{i1}\ a_{11}\ a_{21}\ a_{31} \cdots a_{im}$.

→ The nominal simplify $a_1^{k_1} a_2^{k_2} \cdots a_m^{k_m}$. since There are n binomial $\binom{n}{k_1, k_2, \cdots k_m}$

ways to make those choice the coefficent of $a_1^{k_1}, a_2^{k_2} \cdots a_m^{k_m}$ is $\binom{n}{k_1, k_2 \cdots k_m}$

Application of inclusion and exclusion principle:

→ let x_i be the subset containing the elements that have property P_i. The no. of elements with all properties $P_{i_1}, P_{i_2}, \cdots P_{i_k}$.

→ Then we have $|x_{i_1} \cap x_{i_2} \cap \cdots \cap x_{i_k}| = N(P_{i_1}, P_{i_2} \cdots P_{i_k})$

if the number of elements with none of the properties $P_1, P_2 \cdots P_n$ is denoted

$N = (P_1', P_2' \cdots P_n')$ and the number of elements in the set is denoted by N

Then $N(P_1', P_2' \cdots P_n') = N - |x_1 \cup x_2 \cup x_3 \cdots x_n|$

by the principle inclusion and exclusion we have

$$N(P_1', P_2' \cdots P_n') = N - \sum_{1 \le i \le n} N(P_i)$$

$$+ \sum_{1 \le i \le J \le n} N(P_i P_J) - \sum_{1 \le i \le J \le k \le n} N(P_i P_J P_k)$$

$$+ \cdots + (-1)^n N(P_1 P_2 \cdots P_n)$$

1. find the no. of primes not exceeding 100 and not divisible by 2, 3, 5 or 7

2. How many solutions does $x_1 + x_2 + x_3 = 11$ have where x_1, x_2, x_3 are non negative integers with $x_1 \le 3$, $x_2 \le 4$ and $x_3 \le 6$

3. find the number of integer solution of $x_1 + x_2 + x_3 + x_4 + x_5 = 30$ where

$x_1 \geq 2$, $x_2 \geq 3$, $x_3 \geq 4$, $x_4 \geq 2$, $x_5 \geq 0$.

④ find the no. of positive integers where ~~n~~ n, where $1 \leq n \leq 2000$ & n is not divisible by 2, 3, 0r 5 but is divisible by ⑦.

<u>1 sol</u>: let, P_1 be the property that an integer is divisible by 2

let P_2 be the property that an integer is divisible by 3

let P_3 be the property that an integer is divisible by 5

let P_4 be the property that an integer is divisible by 7

The no. of positive integers not exceeding 100. that are not divisible by 2, 3, 5, 7 is

$$N(P_1' P_2' P_3' P_4') = N - N(P_1 P_2 P_3 P_4)$$

$$= N - [N(P_1) + N(P_2) + N(P_3) + N(P_4) - N(P_1 P_2) - N(P_1 P_3)$$

$$- N(P_1)(P_4) - N(P_2 P_3) - N(P_2, P_4) - N(P_3 P_4)$$

$$+ N(P_3 P_4 P_1)$$

$$+ N(P_2 P_3 P_4) + N(P_1 P_2 P_3) + N(P_1 P_2 P_4) - N(P_1 P_2 P_3 P_4)$$

$N = 99$

$$\Rightarrow 99 - \left[\left\lfloor \frac{100}{2} \right\rfloor + \left\lfloor \frac{100}{3} \right\rfloor + \left\lfloor \frac{100}{5} \right\rfloor + \left\lfloor \frac{100}{7} \right\rfloor - \left\lfloor \frac{100}{2\times3} \right\rfloor - \left\lfloor \frac{100}{2\times5} \right\rfloor - \left\lfloor \frac{100}{2\times7} \right\rfloor - \left\lfloor \frac{100}{3\times5} \right\rfloor - \left\lfloor \frac{100}{2\cdot7} \right\rfloor - \left\lfloor \frac{100}{5\cdot7} \right\rfloor + \left\lfloor \frac{100}{2\times3\times5} \right\rfloor + \left\lfloor \frac{100}{3\times5\times7} \right\rfloor + \left\lfloor \frac{100}{5\times7\times2} \right\rfloor + \left\lfloor \frac{100}{2\times3\times7} \right\rfloor - \left\lfloor \frac{100}{2\cdot3\cdot5\cdot7} \right\rfloor \right]$$

$\Rightarrow 99 - 78$

$\Rightarrow 21$

Thus The no of integers not exceeding (100) that are divisible by none of 2, 3, 5, 7 is '21'. Hence the no of primes not exceeding 100 is $21 + 4 \Rightarrow 25$

(4)

Sol:- let P_1 be the property that 'n' is divisible by 2

let P_2 be the property that 'n' is divisible by 3

let P_3 be the property that n is divisible by 5

let P_4 be the property that n is divisible by 7

Now the number +ve integer n $1 \le n < 2000$ That are divisible by 2, 3, 5 is.

$N(P_1'P_2'P_3') = N - (N(P_1) + N(P_2) + N(P_3) - N(P_1P_2) -$

$N(P_2P_3) - N(P_3P_1) + N(P_1P_2P_3))$

$$= 2000 - \left[\left\lfloor\frac{2000}{2}\right\rfloor + \left\lfloor\frac{2000}{3}\right\rfloor + \left\lfloor\frac{2000}{5}\right\rfloor - \left\lfloor\frac{2000}{2\times3}\right\rfloor - \left\lfloor\frac{2000}{3\times5}\right\rfloor - \left\lfloor\frac{2000}{3\times2}\right\rfloor + \left\lfloor\frac{2000}{2\times3\times5}\right\rfloor\right]$$

$$= 2000 - [1000 + 666 + 400 - 333 - 200 - 133 + 66]$$

$$= 534$$

Hence the number of positive integer $1 \le n \le 2000$ that are not divisible by 2, 3, 5 but are divisible by '7' Is.

$$534/7 = 76.$$

(2)

Sol:- let P_1 be the property $x_1 > 3$,

P_2 be the property $x_2 > 4$

P_3 be the property $x_3 > 6$;

The Number of solutions satisifying The Equation $x_1 \le 3, x_2 \le 4, x_3 \le 6$ is

$N(P_1'P_2'P_3') = N - [n(P_1) + n(P_2) + n(P_3) - n(P_1P_2)$

$- n(P_2P_3) - n(P_3P_1) + n(P_1P_2P_3)]$

Where N is, the total no.of solutions.

$\Rightarrow {}^{n+r-1}C_r$,

Here $n=3$, $r=11$

$\rightarrow {}^{3+11-1}C_{11}$

${}^{14-1}C_{11}$

$${}^{13}C_{11} \Rightarrow \frac{13!}{2!\ 11!}$$

$$= \frac{13 \times \overset{6}{\cancel{12}} \times \cancel{11 \times 10 \times 9 \times 8 \times 7 \times 6 \times 5 \times 4 \times 3 \times 2 \times 1}}{\cancel{2}!\ \cancel{\times 11 \times 10 \times 9 \times \cdots} \times 1}$$

$N = 78$

$\rightarrow N(P_1)$ is the Number of solutions ~~wit~~ is $x_1 \geq 4$

$n=3$, $r=7$

${}^{n+r-1}C_r$

${}^{3+7-1}C_7$

${}^{10-1}C_7$

${}^{9}C_7$

$$\Rightarrow \frac{9 \times 8 \times \cancel{7 \times 6 \times 5 \times 4 \times 3 \times 2 \times 1}}{(9-7)!\ \cancel{7 \times 6 \times 5 \times 4 \times 3 \times 2 \times 1}}$$

$$\Rightarrow \frac{9 \times \overset{4}{\cancel{8}} \times \cancel{7}}{\cancel{2} \times 1} \Rightarrow 36$$

$\Rightarrow N(P_2)$ is the Number of solutions is $x_2 \geq 5$

$n=3$, $r=6$

${}^{n+r-1}C_r$

${}^{3+6-1}C_6 \Rightarrow {}^{8}C_6$

$$\frac{\overset{4}{\cancel{8}}\times 7\times \cancel{6\times 5\times 4\times 3\times 2\times 1}}{\cancel{2}!\ \cancel{6\times 5\times 4\times 3\times 2\times 1}} \Rightarrow 28$$

$\Rightarrow N(P_3)$ is the Number of solutions is $x_3 \geq 7$

$n=3,\ r=4$

$n+r-1C_r$

$3+4-1C_4$

$7-1C_4$

$6C_4$

$$\Rightarrow \frac{\overset{3}{\cancel{6}}\times 5\times \cancel{4\times 3\times 2\times 1}}{\cancel{2}!\times \cancel{4\times 3\times 2\times 1}}$$

$\Rightarrow 15$

$N(P_1P_2)$ The number of solutions is

$x_1 \geq 4,\ x_2 \geq 5$

Here, $n=3,\ r=2$

$n+r-1C_r = 3+2-1C_2 = 5-1C_2 = 4C_2$

$$= \frac{\overset{2}{\cancel{4}}\times 3\times \cancel{2\times 1}}{\cancel{2}!\ \cancel{2\times 1}} = 6.$$

$N(P_2P_3)$ The Number of solution is

$x_2 \geq 5 \quad x_3 \geq 7$

Here $n=3$.

$\therefore\ x_2+x_3 = 12$ but total solutions are 11

$\therefore$ no solutions in this case '0'.

$n(P_2 P_3) = 0.$

$N(P_3P_1)$ The number of solution is

$x_3 \geq 7,\ x_1 \geq 4,\ 3c_0 = \frac{3!}{3!\,0!} = 3+0-1c_0 = 2c_0$

Here $n=3, r=0$

$x_3 + x_1 = 11$ but total solutions are Equal.

$\therefore$ solutions in this case

$\therefore n(P_3 - P_1) = 0$

$n(P_1P_2P_3)$ The number of solutions is

$x_1 \geq 4 \quad x_2 \geq 5 \quad x_3 \geq 6$

$N(P_1' P_2' P_3') = 78 - [36 + 28 + 15 - 6 - 1 - 0 + 0]$

$= 78 - 72$

$= 6.$

<u>Pigeon</u> <u>hole</u> <u>principle</u>:

if n objects are placed into m boxes and $n>m$ then there is Atleast one box that contains two or more objects

<u>generalized</u> <u>pigeon hole</u> <u>principle</u>:-

if 'N' objects are placed into k boxes then there is Atleast one box containing $\frac{N}{k}$ objects (or)

if 'N' objects are placed into 'k' boxes and $N>k$ then atleast one of the pigeon hole must contain $\left[\frac{N-1}{k}\right]+1$ objects

M(200) people How many of them was born on the same month

Sol: since there are 12 months in year the Number of people born on the same month

Here $N = 200$, $k = 12$ months

By pigeon hole principle $\left[\frac{N-1}{k}\right]+1$

$$= \left[\frac{200-1}{12}\right]+1 = \frac{199}{12}+1$$

$= 17$

In how many ways can 20 similar books be placed on 5 different shelves,

since there are 20 similar books

$n = 20$, $k = 5$

by pigeon hole principle $\left[\frac{N-1}{k}\right]+1$

$$= \frac{20-1}{5}+1$$

$$= \frac{19}{5}+1 \Rightarrow 4.8 \text{ or } 5.$$

In how many ways can three different coins be placed in two different purses.

since there are 3 diff coins.

$N = 3$, $k = 2$

by Pigeon hole principle $\left[\frac{N-1}{k}\right]+1$

$$= \frac{3-1}{2}+1$$

$$= \frac{2}{2}+1 = \underline{\underline{2}}$$

Number Theory

Properties of Integers

Let us denote the set of natural numbers (also called positive integers)by N and the set of integers by Z.
i.e., $N = \{1, 2, 3...\}$ and $Z = \{...., -2, -1, 0, 1, 2...\}$.
The following simple rules associated with addition and multiplication of these inte-gers are given below:
(a). Associative law for multiplication and addition

$(a + b) + c = a + (b + c)$ and $(ab)c = a(bc)$, for all $a, b, c \in Z$.

(b). Commutative law for multiplication and addition $a + b = b + a$ and $ab = ba$, for all $a, b \in Z$.

(c). Distritbutive law $a(b + c) = ab + ac$ and $(b + c)a = ba + ca$, for all $a, b, c \in Z$.

(d). Additive identity 0 and multiplicative identity 1

$a + 0 = 0 + a = a$ and $a.1 = 1.a = a$, for all $a \in Z$.

(e). Additive inverse of $-a$ for any integer a

$a + (-a) = (-a) + a = 0$.

Definition: Let a and b be any two integers. Then a is said to be greater than b if $a - b$ is positive integer and it is denoted by $a > b$. $a > b$ can also be denoted by $b < a$.

Basic Properties of Integers

Divisor: A non-zero integer a is said to be *divisor* or *factor* of an integer b if there exists an integer q such that $b = aq$.
If a is divisor of b, then we will write a/b (read as a is a divisor of b). If a is divisor of b, then we say that b is divisible by a or a is a factor of b or b is multiple of a. Examples:
(a). $2/8$, since $8 = 2 \times 4$.
(b). $-4/16$, since $16 = (-4) \times (-4)$.
(c). $a/0$ for all $a \in Z$ and $a \neq 0$, because $0 = a.0$.

Theorem: Let $a, b, c \in Z$, the set of integers. Then,
(i). If a/b and $b \neq 0$, then $|a| \leq |b|$.
(ii). If a/b and b/c, then a/c.
(iii). If a/b and a/c, then $a/b + c$ and $a/b - c$.
(iv). If a/b, then for any integer m, a/bm.
(v). If a/b and a/c, then for any integers m and n, $a/bm + cn$.
(vi). If a/b and b/a then $a = \pm b$.
(vii). If a/b and $a/b + c$, then a/c.
(viii). If a/b and $m \neq 0$, then ma/mb.
Proof:
(i). We have $a/b \Rightarrow b = aq$, where $q \in Z$.

Since $b \neq 0$, therefore $q \neq 0$ and consequently $|q| \geq 1$.

Also, $|q| \geq 1 \Rightarrow |a||q| \geq |a|$

$\Rightarrow |b| \geq |a|$.

(ii). We have $a/b \Rightarrow b = aq_1$, where $q_1 \in Z$.

$b/c \Rightarrow c = bq_2$, where $q_2 \in Z$.

$\therefore c = bq_2 = (aq_1)q_2 = a(q_1q_2) = aq$, where $q = q_1q_2 \in Z. \Rightarrow a/c$.

(iii). We have $a/b \Rightarrow b = aq_1$, *where* $q_1 \in Z$.

$a/c \Rightarrow c = aq_2$, where $q_2 \in Z$.

Now $b + c = aq_1 + aq_2 = a(q_1 + q_2) = aq$, where $q = q_1 + q_2 \in Z$.

$\Rightarrow a/b + c$.

Also, $b - c = aq_1 - aq_2 = a(q_1 - q_2) = aq$, where $q = q_1 - q_2 \in Z$.

$\Rightarrow a/b - c$.

(iv). We have $a/b \Rightarrow b = aq$, where $q \in Z$.

For any integer m, $bm = (aq)m = a(qm) = aq$, where $a = qm \in Z$.

$\Rightarrow a/bm$.

(v). We have $a/b \Rightarrow b = aq_1$, where $q_1 \in Z$.

$a/c \Rightarrow c = aq_2$, where $q_2 \in Z$.

Now $bm + cn = (aq_1)m + (aq_2)n = a(q_1m + q_2n) = aq$, where $q = q_1m + q_2n \in Z$

$\Rightarrow a/mb + cn$.

(vi). We have $a/b \Rightarrow b = aq_1$, where $q_1 \in Z$.

$b/a \Rightarrow a = bq_2$, where $q_2 \in Z$.

$\therefore b = aq_1 = (bq_2)q_1 = b(q_2q_1)$

$\Rightarrow b(1 - q_2q_1) = 0$

$q_2q_1 = 1 \Rightarrow q_2 = q_1 = 1$ or $q_2 = q_1 = -1$

$\therefore a = b$ or $a = -b$ i.e., $a \pm b$. (vii). We have $a/b \Rightarrow b$

$= aq_1$, where $q_1 \in Z$.

$a/b + c \Rightarrow b + c = aq_2$, where $q_2 \in Z$

Now, $c = b - aq_2 = aq_1 - aq_2 = a(q_1 - q_2) = aq$, where $q = q_1 - q_2 \in Z$.

$\Rightarrow a/c$.

(viii). We have $a/b \Rightarrow b = aq_1$, where $q_1 \in Z$.

Since $m \neq 0$, $mb = m(aq_1) = ma(q_1)$

$\Rightarrow ma/mb$.

Greatest Common Divisor (GCD)

Common Divisor: A non-zero integer d is said to be a *common divisor* of integers a and b if d/a and d/b.

Example:

(1). $3/-15$ and $3/21 \Rightarrow 3$ is a common divisor of 15, 21.

(2). ± 1 is a common divisor of a, b, where $a, b \in Z$.

Greatest Common Divisor: A non-zero integer d is said to be a *greatest common divisor* (gcd) of a and b if

(i). d is a common divisor of a and b; and

(ii). every divisor of a and b is a divisor of d.

We write $d = (a, b)$=gcd of a, b.

Example: 2, 3 and 6 are common divisors of 18, 24.

Also 2/6 and 3/6. Therefore 6 = (18, 24).

Relatively Prime: Two integers a and b are said to be *relatively prime* if their greatest common divisor is 1, i.e., gcd(a, b)=1.

Example: Since (15, 8) = 1, 15 and 8 are relatively prime.

Note:

(i). If a, b are relatively prime then a, b have no common divisors.

(ii). $a, b \in Z$ are relatively prime iff there exists $x, y \in Z$ such that $ax + by = 1$.

Basic Properties of Greatest Common Divisors:

(1). If c/ab and gcd(a, c) = 1 then c/b.

Solution: We have $c/ab \Rightarrow ab = cq_1, q_1 \in Z.$

$(a, c) = 1 \Rightarrow$ there exist $x, y \in Z$ such that

$ax + cy = 1.$

$ax + cy = 1 \Rightarrow b(ax + cy) = b$

$\Rightarrow (ba)x + b(cy) = b \Rightarrow (cq_1)x + b(cy) = b \Rightarrow c[q_1x + by] = b$

$\Rightarrow cq = b$, where $q = q_1x + by \in Z \Rightarrow c/b.$

(2). If $(a, b) = 1$ and $(a, c) = 1$, then $(a, bc) = 1$.

Solution: $(a, b) = 1$, there exist $x_1, y_1 \in Z$ such that

$ax_1 + by_1 = 1$

$\Rightarrow by_1 = 1 - ax_1$——————-(1)

$(a, c) = 1$, there exist $x_2, y_2 \in Z$ such that

$ax_2 + by_2 = 1$

$\Rightarrow cy_2 = 1 - ax_2$——————-(2)

From (1) and (2), we have

$(by_1)(cy_2) = (1 - ax_1)(1 - ax_2)$

$\Rightarrow bcy_1y_2 = 1 - a(x_1 + x_2) + a^2x_1x_2 \Rightarrow a(x_1 + x_2 - ax_1x_2) + bc(y_1y_2) = 1$

$\Rightarrow ax_3 + bcy_3 = 1$, where $x_3 = x_1 + x_2 - ax_1x_2$ and $y_3 = y_1y_2$ are integers.

$\therefore$ There exists $x_3, y_3 \in Z$ such that $ax_3 + bcy_3 = 1$.

(3). If $(a, b) = d$, then $(ka, kb) = |k|d.$, k is any integer.

Solution: Since $d = (a, b) \Rightarrow$ there exist $x, y \in Z$ such that

$ax + by = d.$

$\Rightarrow k(ax) + k(by) = kd \Rightarrow (ka)x + (kb)y = kd$

$\therefore (ka, kb) = kd = k(a, b)$

(4). If $(a, b) = d$, then $(\frac{a}{d}, \frac{b}{d}) = 1$.

Solution: Since $(a, b) = d \Rightarrow$ there exist $x, y \in Z$ such that $ax + by = d$.

$$\Rightarrow (ax+by)/d = 1$$

$$\Rightarrow (a/d)x + (b/d)y = 1$$

Since d is a divisor of both a and b, a/d and b/d are both integers.
Hence (a/d,b/d) = 1.

Division Theorem (or Algorithm)

Given integers a and d are any two integers with $b > 0$, there exist a unique pair of integers q and r such that $a = dq + r$, $0 \leq r < b$. The integer's q and r are called the quotient and the remainder respectively. Moreover, $r = 0$ if, and only if, $b|a$.

Proof:

Consider the set, S, of all numbers of the form a+nd, where n is an integer.

S = {a - nd : n is an integer}

S contains at least one nonnegative integer, because there is an integer, n, that ensures a-nd $\geq$ 0, namely

n = -|a| d makes a-nd = a+|a| $d^2 \geq$ a+|a| $\geq$ 0.

Now, by the well-ordering principle, there is a least nonnegative element of S, which we will call r, where r=a-nd for some n. Let q = (a-r)/d = (a-(a-nd))/d = n. To show that r < |d|, suppose to the contrary that r $\geq$ |d|. In that case, either r-|d|=a-md, where m=n+1 (if d is positive) or m=n-1 (if d is negative), and so r-|d| is an element of S that is nonnegative and smaller than r, a contradiction. Thus r < |d|.

To show uniqueness, suppose there exist q,r,q',r' with 0 $\leq$ r,r' < |d|

such that a=qd + r and a =q'd + r'.

Subtracting these equations gives d(q'-q) = r'-r, so d|r'-r. Since 0 $\leq$ r,r' < |d|, the difference r'-r must also be smaller than d. Since d is a divisor of this difference, it follows that the difference r'-r must be zero, i.e. r'=r, and so q'=q.

Example: If $a = 16$, $b = 5$, then $16 = 3 \times 5 + 1$; $0 \leq 1 < 5$.

Euclidean Algorithm for finding the GCD

An efficient method for finding the greatest common divisor of two integers based on the quotient and remainder technique is called the Euclidean algorithm. The following lemma provides the key to this algorithm.

Lemma: If $a = bq + r$, where a, b, q and r are integers, then gcd(a, b)=gcd(b, r).

Statement: When a and b are any two integers ($a > b$), if r_1 is the remainder when a is divided by b, r_2 is the remainder when b is divided by r_1, r_3 is the remainder when r_1 is divided by r_2 and so on and if $r_{k+1} = 0$, then the last non-zero remainder r_k is the gcd(a, b).

Proof:

By the unique division principle, a divided by b gives quotient q and remainder r,

such that $a = bq+r$, with $0 \leq r < |b|$.

Consider now, a sequence of divisions, beginning with a divided by b giving quotient q_1 and remainder b_1, then b divided by b_1 giving quotient q_2 and remainder b_2, etc.

$a=bq_1+b_1$,
$b=b_1q_2+b_2$,
$b_1=b_2q_3+b_3$,
...
$b_{n-2}=b_{n-1}q_n+b_n$,
$b_{n-1}=b_nq_{n+1}$

In this sequence of divisions, $0 \leq b_1 < |b|$, $0 \leq b_2 < |b_1|$, etc., so we have the sequence $|b| > |b_1| > |b_2| > ... \geq 0$. Since each b is strictly smaller than the one before it, eventually one of them will be 0. We will let b_n be the last non-zero element of this sequence.

From the last equation, we see $b_n \mid b_{n-1}$, and then from this fact and the equation before it, we see that $b_n \mid b_{n-2}$, and from the one before that, we see that $b_n \mid b_{n-3}$, etc. Following the chain backwards, it follows that $b_n \mid b$, and $b_n \mid a$. So we see that b_n is a common divisor of a and b.

To see that b_n is the *greatest* common divisor of a and b, consider, d, an arbitrary common divisor of a and b. From the first equation, $a-bq_1=b_1$, we see $d|b_1$, and from the second, equation, $b-b_1q_2=b_2$, we see $d|b_2$, etc. Following the chain to the bottom, we see that $d|b_n$. Since an arbitrary common divisor of a and b divides b_n, we see that b_n is the greatest common divisor of a and b.

Example: Find the gcd of 42823 and 6409.

Solution: By Euclid Algorithm for 42823 and 6409, we have

42823= 6.6409+ 4369, r1= 4369,
6409= 1.4369+2040, r2= 2040,
4369= 2.2040+289, r3 = 289,
2040= 7.289+ 17, r4 = 17,
289= 17.17+ 0,
r5 = 0

$\therefore r_4 = 17$ is the last non-zero remainder. $\therefore d = (42823, 6409) = 17$.

Example: Find the gcd of 826, 1890.
Solution: By Euclid Algorithm for 826 and 1890, we have

1890= 2.826+ 238,r1= 238
826= 3.238+ 112,r2= 112
238= 2.112+ 14,r3 = 14
112= 8.14 + 0, r4 = 0

$\therefore r_3 = 14$ is the last non-zero remainder. $\therefore d = (826, 1890) = 14$.

****Example: Find the gcd of 615 and 1080, and find the integers x and y such that gcd(615, 1080) = $615x + 1080y$.
Solution: By Euclid Algorithm for 615 and 1080, we have

$$1080 = 1.615 + 465, \ r_1 = 465 - - - - - (1)$$

$$615 = 1.465 + 150, \ r_2 = 150 - - - - - (2)$$

$465 = 3.150 + 15, \ r_3 = 15 - - - - - - (3)$

$150 = 10.15 + 0, \ r_4 = 0 - - - - - - - - (4)$

$\therefore r_3 = 15$ is the last non-zero remainder.

$\therefore d = (615, 1080) = 15$. Now, we find x and y such that

$615x + 1080y = 15$.
To find x and y, we begin with last non-zero remainder as follows.
$d = 15 = 465 + (-3).150$; using (3)

$=465 + (-3)\{615 + (-1)465\}$; using (2)
$=(-3).615 + (4).465$
$=(-3).615 + 4\{1080 + (-1).615\}$; using (1)
$=(-7).615 + (4).1080$
$=615x + 1080y$

Thus gcd(615, 1080) = 15 provided $15 = 615x + 1080y$, where $x = -7$ and $y = 4$.
Example: Find the gcd of 427 and 616 and express it in the form $427x + 616y$.
Solution: By Euclid Algorithm for 427 and 616, we have

616= 1.427+189,r1 = 189.........(1)
427= 2.189+49,r2 = 49............(2)
189= 3.49+ 42, r3 = 42..............(3)
49= 1.42+ 7,r4 = 7..................(4)
42= 6.7 + 0,r5 = 0....................(5)

$\therefore r_5 = 7$ is the last non-zero remainder.

$\therefore d = (427, 616) = 7$. Now, we find x and y such that

$427x + 616y = 7$.
To find x and y, we begin with last non-zero remainder as follows.
$d = 7 = 49 + (-1).42$; using (4)

$=49 + (-1)\{189 + (-3).49\}$; using (3)
$=4.49 - 189$
$=4.\{427 + (-2).189\} - 189$; using (2)
$=4.427 + (-8).189 - 189$
$=4.427 + (-9).189$
$=4.427 + (-9)\{616 + (-1)427\}$; using (1)
$=4.427 + (-9).616 + 9.427$
$=13.427 + (-9).616$

Thus gcd(427, 616) = 7 provided $7 = 427x + 616y$, where $x = 13$ and $y = -9$.
Example: For any positive integer n, prove that the integers $8n + 3$ and $5n + 2$ are relatively prime.
Solution: If $n = 1$, then gcd($8n + 3, 5n + 2$)=gcd(11, 7) = 1.
If $n \geq 2$, then we have $8n + 3 > 5n + 2$, so we may write
$8n + 3 = 1.(5n + 2) + 3n + 1,\quad 0 < 3n + 1 < 5n + 2$
$5n + 2 = 1.(3n + 1) + 2n + 1,\quad 0 < 2n + 1 < 3n + 1$
$3n + 1 = 1.(2n + 1) + n,\quad 0 < n < 2n + 1$
$2n + 1 = 2.n + 1,\quad 0 < 1 < n$
$n = n.1 + 0.$
Since the last non-zero remainder is 1, gcd($8n + 3, 5n + 2$) = 1 for all $n \geq 1$.
Therefore the given integers $8n + 3$ and $5n + 2$ are relatively prime.
Example: If $(a, b) = 1$, then $(a + b, a - b)$ is either 1 or 2.

Solution: Let $(a + b, a - b) = d \Rightarrow d|a + b, d|a - b$.

Then $a + b = k_1d$........(1)

and $a - b = k_2d$..........(2)

Solving (1) and (2), we have

$2a = (k_1 + k_2)d$ and $2b = (k_1 - k_2)d$

$\therefore d$ divides $2a$ and $2b$

$\therefore d \leq$gcd($2a, 2b$) = 2 gcd(a, b) = 2, since gcd(a, b) = 1 $\therefore d = 1$ or 2.

Then $2a + b = k_1d$........ (1)

and $a + 2b = k_2d$.......... (2)

$3a = (2k_1 - k_2)d$ and $3b = (2k_2 - k_1)d$

$\therefore d$ divides $3a$ and $3b$

$\therefore d \leq$gcd($3a, 3b$) = 3 gcd(a, b) = 3, since gcd(a, b) = 1 $\therefore d = 1$ or 2 or 3.

But d cannot be 2, since $2a + b$ and $a + 2b$ are not both even [when a is even and b is odd, $2a + b$ is odd and $a + 2b$ is even; when a is odd and b is even, $2a + b$ is even and $a + 2b$ is odd; when both a and b are odd $2a + b$ and $a + 2b$ are odd.] Hence $d = (2a + b, a + 2b)$ is 1 or 3.

Least Common Multiple (LCM)

Let a and b be two non-zero integers. A positive integer m is said to be a *least common multiple* (lcm) of a and b if

(i) m is a common multiple of a and b i.e., a/m and b/m,

and

(ii) c is a common multiple of a and b, c is also a multiple of m

i.e., if a/c and b/c, then m/c.

In other words, if a and b are positive integers, then the smallest positive integer that is divisible by both a and b is called the least common multiple of a and b and is denoted by lcm(a, b).
Note: If either or both of a and b are negative then lcm(a, b) is always positive.
Example: lcm(5, -10)=10, lcm(16, 20)=80.

Prime Numbers

Definition: An integer n is called prime if $n > 1$ and if the only positive divisors of n are 1 and n. If $n > 1$ and if n is not prime, then n is called composite.

Examples: The prime numbers less than 100 are 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, and 97.

Theorem: Every integer $n > 1$ is either a prime number or a product of prime numbers.

Proof: We use induction on n. The theorem is clearly true for $n = 2$. Assume it is true for every integer $< n$. Then if n is not prime it has a positive divisor $d \neq 1$, $d \neq n$. Hence $n = cd$, where $c \neq n$. But both c and d are $< n$ and > 1 so each of c, d is a product of prime numbers, hence so is n.

Fundamental Theorem of Arithmetic

Theorem: *Every integer $n > 1$ can be expressed as a product of prime factors in only one way, a part from the order of the factor.*

Proof:

There are two things to be proved. Both parts of the proof will use he Well-ordering Principle for the set of natural numbers.
(1) We first prove that every a > 1 can be written as a product of prime factors. (This includes the possibility of there being only one factor in case a is prime.)
Suppose bwoc that there exists a integer a > 1 such that a cannot be written as a product of primes.
By the Well-ordering Principle, there is a smallest such a.
Then by assumption a is not prime so a = bc where 1 < b, c < a.
So b and c can be written as products of prime factors (since a is the smallest positive integer than cannot be.)
But since a = bc, this makes a a product of prime factors, a contradiction.
(2) Now suppose bwoc that there exists an integer a > 1 that has two different prime factorizations, say a = p1 ··· ps = q1 ··· qt , where the pi and qj are all primes. (We allow repetitions among the pi and qj . That way, we don't have to use exponents.)
Then p1| a = q1 ··· qt . Since p1 is prime, by the Lemma above, p1| qj for some j .
Since qj is prime and p1 > 1, this means that p1 = qj .
For convenience, we may renumber the qj so that p1 = q1 .
We can now cancel p1 from both sides of the equation above to get p2 ··· ps = q2 ··· qt . But p2 ··· ps < a and by assumption a is the smallest positive integer with a non–unique prime factorization.
It follows that s = t and that p2,...,ps are the same as q2,...,qt , except possibly in a different order.
But since p1 = q1 as well, this is a contradition to the assumption that these were two different factorizations.
Thus there cannot exist such an integer a with two different factorizations

Example: Find the prime factorisation of 81, 100 and 289. Solution: $81 = 3 \times 3 \times 3 \times 3 = 3^4$

$100 = 2 \times 2 \times 5 \times 5 = 2^2 \times 5^2$

$289 = 17 \times 17 = 17^2$.

Theorem: Let $m = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$ and $n = p_1^{b_1} p_2^{b_2} \ldots p_k^{b_k}$. Then

$\gcd(m, n) = p_1^{\min(a_1,b_1)} \times p_2^{\min(a_2,b_2)} \times \ldots \times p_k^{\min(a_k,b_k)}$
$= \prod p_i^{\min(a_i,b_i)}$, where $\min(a, b)$ represents the minimum of the two numbers a and b.

$\mathrm{lcm}(m, n) = p_1^{\max(a_1,b_1)} \times p_2^{\max(a_2,b_2)} \times \ldots \times p_k^{\max(a_k,b_k)}$
$= \prod p_i^{\max(a_i,b_i)}$, where $\max(a,b)$ represents the maximum of the two numbers a and b.

Theorem: If a and b are two positive integers, then $\gcd(a, b).\mathrm{lcm}(a, b) = ab$.

Proof: Let prime factorisation of a and b be

$m = p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k}$ and $n = p_1^{b_1} p_2^{b_2} \ldots p_k^{b_k}$

Then $\gcd(a, b) = p_1^{\min(a_1,b_1)} \times p_2^{\min(a_2,b_2)} \times \ldots \times p_k^{\min(a_k,b_k)}$ and

$\mathrm{lcm}(m, n) = p_1^{\max(a_1,b_1)} \times p_2^{\max(a_2,b_2)} \times \ldots \times p_k^{\max(a_k,b_k)}$

We observe that if $\min(a_i, b_i)$ is a_i(or b_i) then $\max(a_i, b_i)$ is b_i(or a_i), $i = 1, 2.., n$.

Hence $\gcd(a, b).\mathrm{lcm}(a, b)$

$$= p_1^{\min(a_1,b_1)} \times p_2^{\min(a_2,b_2)} \times \ldots \times p_k^{\min(a_k,b_k)} \times p_1^{\max(a_1,b_1)}.p_2^{\max(a_2,b_2)} \ldots p_k^{\max(a_k,b_k)}$$

$$= p_1^{[\min(a_1,b_1)+\max(a_1,b_1)]}.p_2^{[\min(a_2,b_2)+\max(a_2,b_2)]} \ldots p_k^{[\min(a_k,b_k)+\max(a_k,b_k)]}$$

$$= p_1^{(a_1+b_1)}.p_2^{(a_2+b_2)} \ldots p_k^{(a_k+b_k)}$$

$$= (p_1^{a_1} p_2^{a_2} \ldots p_k^{a_k})(p_1^{b_1} p_2^{b_2} \ldots p_k^{b_k})$$

$$= ab.$$

Example: Use prime factorisation to find the greatest common divisor of 18 and 30.

Solution: Prime factorisation of 18 and 30 are

$18 = 2^1 \times 3^2 \times 5^0$ and $30 = 2^1 \times 3^1 \times 5^1$.

$\gcd(18, 30) = 2^{\min(1,1)} \times 3^{\min(2,1)} \times 5^{\min(0,1)}$
$= 2^1 \times 3^1 \times 5^0$
$= 2 \times 3 \times 1$
$= 6.$

Example: Use prime factorisation to find the least common multiple of 119 and 544.

Solution: Prime factorisation of 119 and 544 are

$119 = 2^0 \times 7^1 \times 17^1$ and $544 = 2^5 \times 7^0 \times 17^1$.

$\mathrm{lcm}(119, 544) = 2^{\max(0,5)} \times 7^{\max(1,0)} \times 17^{\max(1,1)}$
$= 2^5 \times 7^1 \times 17^1$
$= 32 \times 7 \times 17$
$= 3808.$

Example: Using prime factorisation, find the gcd and lcm of (i). (231, 1575) (ii). (337500, 21600). Verify also gcd(m, n). lcm(m, n) = mn.

Example: Prove that $\log_3 5$ is irrational number.

Solution: If possible, let $\log_3 5$ is rational number.

$\Rightarrow \log_3 5 = u/v$, where u and v are positive integers and prime to each other.

$\therefore 3^{u/v} = 5$

i.e., $3^u = 5^v = n$, say.
This means that the integer $n > 1$ is expressed as a product (or power) of prime numbers (or a prime number) in two ways.
This contradicts the fundamental theorem arithmetic.

$\therefore \log_3 5$ is irrational number.

Example: Prove that$\sqrt{5}$ is irrational number.
Solution: If possible, let$\sqrt{5}$ is rational number.
$\Rightarrow \sqrt{5} = u/v$, where u and v are positive integers and prime to each other.
$\Rightarrow u^2 = 5v^2$..................(1)
$\Rightarrow u^2$ is divisible by 5
$\Rightarrow u$ is divisible by 5 i.e., $u = 5m$.........(2)
$\therefore$ From (1), we have $5v^2 = 25m^2$ or $v^2 = 5m^2$
i.e., v^2 and hence v is divisible by 5
i.e., $v = 5n$..........(3)
From (2) and (3), we see that u and v have a common factor 5, which contradicts the assumption.
$\therefore \sqrt{5}$ is irrational number.

Testing of Prime Numbers

Theorem: If $n > 1$ is a composite integer, then there exists a prime number p such that p/n and $p \leq \sqrt{n}$.
Proof: Since $n > 1$ is a composite integer, n can be expressed as $n = ab$, where $1 < a \leq b < n$. Then $a \leq \sqrt{n}$.
If $a > \sqrt{n}$, then $b \geq a > \sqrt{n}$.
$\therefore$ $n = ab > \sqrt{n}.\sqrt{n} = n$, i.e. $n > n$, which is a contradiction.
Thus n has a positive divisor (= a) not exceeding$\sqrt{n}$.
$a > 1$, is either prime or by the Fundamental theorem of arithmetic, has a primefactor. In ither ase, n has a prime factor$\leq\sqrt{n}$.

Algorithm to test whether an integer $n > 1$ is prime:

Step 1: Verify whether n is 2. If n is 2, then n is prime. If not goto step 2.
Step 2: Verify whether 2 divides n. If 2 divides n, then n is not a prime. If 2 does not divides n, then goto step (3).
Step 3: Find all odd primes $p \leq \sqrt{n}$.If there is no such odd prime, then n is prime otherwise, goto step (4).
Step 4: Verify whether p divides n, where p is a prime obtained in step (3). If p divides n, then n is not a prime. If p does not divide n for any odd prime p obtained in step (3), then n is prime.

Example: Determine whether the integer 113 is prime or not.
Solution: Note that 2 does not divide 113. We now find all odd primes p such that $p^2 \leq 113$.
These primes are 3, 5 and 7, since $7^2 < 113 < 11^2$.
None of these primes divide 113.
Hence, 113 is a prime.

Example: Determine whether the integer 287 is prime or not.
Solution: Note that 2 does not divide 287. We now find all odd primes p such that $p^2 \leq 287$.
These primes are 3, 5, 7, 11 and 13, since $13^2 < 287 < 17^2$.
7 divides 287.
Hence, 287 is a composite integer.

Modular Arithmetic

Congruence Relation

If a and b are integers and m is positive integer, then a is said to be congruent to b modulo m, if m divides $a - b$ or $a - b$ is multiple of m. This is denoted as

$$a \equiv b \pmod{m}$$

m is called the modulus of the congruence, b is called the residue of $a \pmod{m}$. If a is not congruent to b modulo m, then it is denoted by $a \not\equiv b \pmod{m}$.
Example:
(i). $89 \equiv 25 \pmod{4}$, since 89-25=64 is divisible by 4. Consequently 25 is the residue of 89(mod 4) and 4 is the modulus of the congruent.

(ii). $153 \equiv -7 \pmod{8}$, since 153-(-7)=160 is divisible by 8. Thus -7 is the residue of 153(mod 8) and 8 is the modulus of the congruent.

(iii). $24 \not\equiv 3 \pmod{5}$, since 24-3=21 is not divisible by 5. Thus 24 and 3 are incon-gruent modulo 5
Note: If $a \equiv b \pmod{m} \Leftrightarrow a - b = mk$, for some integer k

$\Leftrightarrow a = b + mk$, for some integer k.

Properties of Congruence

Property 1: The relation "Congruence modulo m" is an equivalence relation. i.e., for all integers a, b and c, the relation is

(i) Reflexive: For any integer a, we have $a \equiv a \pmod{m}$

(ii) Symmetric: If $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$

(iii) Transitive: If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.

Proof: (i). Let a be any integer. Then $a - a = 0$ is divisible by any fixed positive integer m. Thus $a \equiv a \pmod{m}$.

$\therefore$ The congruence relation is reflexive.

(ii). Given $a \equiv b(\text{mod } m)$

$\Rightarrow a - b$ is divisible by $m \Rightarrow -(a - b)$ is

divisible by $m \Rightarrow b - a$ is divisible by

m

i.e., $b \equiv a(\text{mod } m)$.

Hence the congruence relation is symmetric.

(iii). Given $a \equiv b(\text{mod } m)$ and $b \equiv c(\text{mod } m)$

$\Rightarrow a - b$ is divisible of m and $b - c$ is divisible by m. Hence $(a - b) + (b - c) = a - c$ is divisible by m

i.e., $a \equiv c(\text{mod } m)$

$\Rightarrow$ The congruence relation is transitive.

Hence, the congruence relation is an equivalence relation.

Property 2: If $a \equiv b(\text{mod } m)$ and c is any integer, then

(i). $a \pm c \equiv b \pm c(\text{mod } m)$

(ii). $ac \equiv bc(\text{mod } m)$.

Proof:

(i). Since $a \equiv b(\text{mod } m) \Rightarrow a - b$ is divisible by m.

Now $(a \pm c) - (b \pm c) = a - b$ is divisible by m.

$\therefore a \pm c \equiv b \pm c(\text{mod } m)$.

(ii). Since $a \equiv b(\text{mod } m) \Rightarrow a - b$ is divisible by m.

Now, $(a - b)c = ac - bc$ is also divisible by m.

$\therefore ac \equiv bc(\text{mod } m)$.

Note: The converse of property (2) (ii) is not true always.

Property 3: If $ac \equiv bc(\text{mod } m)$, then $a \equiv b(\text{mod } m)$ only if $\gcd(c,m) = 1$. In fact, if c is an integer which divides m, and if $ac \equiv bc(\text{mod } m)$, then $a \equiv b \text{ mod}\left[\frac{m}{\gcd(c,m)}\right]$

Proof: Since $ac \equiv bc(\text{mod } m) \Rightarrow ac - bc$ is divisible by m.

i.e., $ac - bc = pm$, where p is an integer.

$\Rightarrow a - b = p\left(\frac{m}{c}\right)$

$\therefore a \equiv b\left[\text{ mod }\left(\frac{m}{c}\right)\right]$, provided that $\frac{m}{c}$ is an integer.

Since c divides m, $\gcd(c, m) = c$.

Hence, $a \equiv b \text{ mod }\left[\frac{m}{\gcd(c,m)}\right]$

But, if $\gcd(c, m) = 1$, then $a \equiv b(\text{mod } m)$.

Property 4: If a, b, c, d are integers and m is a positive integer such that $a \equiv b(\text{mod } m)$ and $c \equiv d(\text{mod } m)$, then

(i). $a \pm c \equiv b \pm d(\text{mod } m)$

(ii). $ac \equiv bd(\text{mod } m)$

(iii). $a^n \equiv b^n(\text{mod } m)$, where n is a positive integer.

Proof: (i). Since $a \equiv b(\text{mod } m) \Rightarrow a - b$ is divisible by m.

Also $c \equiv d(\text{mod } m) \Rightarrow c - d$ is divisible by m.

$\therefore (a - b) \pm (c - d)$ is divisible by m. i.e., $(a \pm c) - (b \pm d)$ is divisible by m. i.e., $a \pm c \equiv b \pm d(\text{mod } m)$.

(ii). Since $a \equiv b(\text{mod } m) \Rightarrow a - b$ is divisible by m.

$\therefore (a - b)c$ is also divisible by m.

$\therefore (c - d)b$ is also divisible by m.

$\therefore (a - b)c + (c - d)b = ac - bd$ is divisible by m. i.e., $ac - bd$ is divisible by m.

i.e., $ac \equiv bd(\text{mod } m)$...........................(1)

(iii). In (1), put $c = a$ and $d = b$. Then, we get

$a^2 \equiv b^2(\text{mod } m)$................(2)

Also $a \equiv b(\text{mod } m)$................(3)

Using the property (ii) in equations (2) and (3), we have $a^3 \equiv b^3(\text{mod } m)$

Proceeding the above process we get

$a^n \equiv b^n(\text{mod } m)$, where n is a positive integer.

Fermat's Theorem

If p is a prime and $(a, p) = 1$ then $a^{p-1} - 1$ is divisible by p i.e., $a^{p-1} \equiv 1 \ (\text{mod } p)$.

Proof

We offer several proofs using different techniques to prove the statement $a^p \equiv a \pmod{p}$. If $\gcd(a, p) = 1$, then we can cancel a factor of a from both sides and retrieve the first version of the theorem.

Proof by Induction

The most straightforward way to prove this theorem is by by applying the induction principle. We fix p as a prime number. The base case, $1^p \equiv 1 \pmod{p}$, is obviously true. Suppose the statement $a^p \equiv a \pmod{p}$ is true. Then, by the binomial theorem,

$$(a+1)^p = a^p + \binom{p}{1}a^{p-1} + \binom{p}{2}a^{p-2} + \cdots + \binom{p}{p-1}a + 1.$$

Note that p divides into any binomial coefficient of the form $\binom{p}{k}$ for $1 \le k \le p-1$. This follows by the definition of the binomial coefficient as $\binom{p}{k} = \frac{p!}{k!(p-k)!}$; since p is prime, then p divides the numerator, but not the denominator.

Taken $\bmod p$, all of the middle terms disappear, and we end up with $(a+1)^p \equiv a^p + 1 \pmod p$. Since we also know that $a^p \equiv a \pmod p$, then $(a+1)^p \equiv a + 1 \pmod p$, as desired.

Example: Using Fermat's theorem, compute the values of

(i) $3^{302} \pmod 5$,

(ii) $3^{302} \pmod 7$ and

(iii) $3^{302} \pmod{11}$.

Solution: By Fermat' s theorem, 5 is a prime number and 5 does not divide 3, we have

$$3^{5-1} \equiv 1 \pmod 5$$

$$3^4 \equiv 1 \pmod 5$$

$$(3^4)^{75} \equiv 1^{75} \pmod 5$$

$$3^{300} \equiv 1 \pmod 5$$

$$3^{302} \equiv 3^2 = 9 \pmod 5$$

$$3^{302} \equiv 4 \pmod 5 \text{.............(1)}$$

Similarly, 7 is a prime number and 7 does not divide 3, we have

$$3^6 \equiv 1 \pmod 7$$

$$(3^6)^{50} \equiv 1^{50} \pmod 7$$

$$3^{300} \equiv 1 \pmod 7$$

$$3^{302} \equiv 3^2 = 9 \pmod 7$$

$$3^{302} \equiv 2 \pmod 7 \text{.............(2)}$$

and 11 is a prime number and 11 does not divide 3, we have

$$3^{10} \equiv 1 \pmod{11}$$

$$(3^{10})^{30} \equiv 1^{30} \pmod{11}$$

$$3^{300} \equiv 1 \pmod{11}$$

$$3^{302} \equiv 3^2 = 9 \pmod{11} \text{.............(3)}$$

Example: Using Fermat's theorem, find $3^{201} \pmod{11}$.

Example: Using Fermat's theorem, prove that $4^{13332} \equiv 16 \pmod{13331}$. Also, give an example to show that the Fermat theorem is true for a composite integer. Solution:

(i). Since 13331 is a prime number and 13331 does not divide 4.

By Fermat's theorem, we have

$$4^{13331-1} \equiv 1 \pmod{13, 331}$$

$$4^{13330} \equiv 1 \pmod{13, 331}$$

$$4^{13331} \equiv 4 \pmod{13, 331}$$

$$4^{13332} \equiv 16 \pmod{13, 331}$$

(ii). Since 11 is prime and 11 does not divide 2.

By Fermat's theorem, we have

$2^{11-1} \equiv 1 \pmod{11}$

i.e., $2^{10} \equiv 1 \pmod{11}$

$(2^{10})^{34} \equiv 1^{34} \pmod{11}$

$2^{340} \equiv 1 \pmod{11}$.............(1)

Also,

$2^5 \equiv 1 \pmod{31}$

$(2^5)^{68} \equiv 1^{68} \pmod{31}$

$2^{340} \equiv 1 \pmod{31}$.............(2)

From (1) and (2), we get

$2^{340} - 1$ is divisible by $11 \times 31 = 341$, since $\gcd(11, 31) = 1$.

i.e., $2^{340} \equiv 1 \pmod{341}$.

Thus, even though 341 is not prime, Fermat theorem is satisfied.

Euler's totient Function:

Euler's totient function counts the positive integers up to a given integer n that are relatively prime to n. It is written using the Greek letter phi as $\phi(n)$, and may also be called Euler's phi function. It can be defined more formally as the number of integers k in the range $1 \le k \le n$ for which the greatest common divisor gcd(n, k) is equal to 1. The integers k of this form are sometimes referred to as totatives of n.

Computing Euler's totient function:

$$\phi(n) = n \prod_{p \mid n}\left(1 - \frac{1}{p}\right)$$

$$= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right),$$

where the product is over the distinct prime numbers dividing

Example: Find $\phi(21)$, $\phi(35)$, $\phi(240)$

Solution:

$$\phi(21) = \phi(3 \times 7)$$
$$= 21\,(1-\frac{1}{3})(1-\frac{1}{7})$$
$$= 12$$

$$\phi(35) = \phi(5 \times 7)$$
$$= 35\,(1-\frac{1}{5})(1-\frac{1}{7})$$
$$= 24$$

$$\phi(240) = \phi(15 \times 16)$$

$$=\phi(3\times5\times 2^4)$$
$$=240\ (1-\frac{1}{3})(1-\frac{1}{5})(1-\frac{1}{2})$$
$$= 64$$

Euler's Theorem: If a and $n > 0$ are integers such that $(a, n) = 1$ then $a^{\phi(n)} \equiv 1 (\text{mod } n)$.
Proof:

Consider the elements $r_1, r_2, \ldots, r_{\phi(n)}$ of (Z/n) the congruence classes of integers that are relatively prime to n.

For $a \in$ (Z/n) the claim is that multiplication by a is a permutation of this set; that is, the set { $ar_1, ar_2, \ldots, ar_{\phi(n)}$ } equals (Z/n). The claim is true because multiplication by a is a function from the finite set (Z/n) to itself that has an inverse, namely multiplication by 1/a (mod n)

Now, given the claim, consider the product of all the elements of (Z/n), on one hand, it is $r_1\, r_2, \ldots r_{\phi(n)}$. On the other hand, it is $ar_1\, ar_2 \ldots ar_{\phi(n)}$. So these products are congruent mod n

$$r_1\, r_2 \ldots r_{\phi(n)} \equiv ar_1\, ar_2 \ldots ar_{\phi(n)}$$

$$r_1\, r_2 \ldots r_{\phi(n)} \equiv \; a^{\phi(n)}\, r_1\, r_2 \ldots r_{\phi(n)}$$

$$1 \equiv a^{\phi(n)}$$

where, cancellation of the r_i is allowed because they all have multiplicative inverses(mod n)

Example: Find the remainder 29^{202} when divided by 13.

Solution: We first note that (29,13)=1.

Hence we can apply Euler's Theorem to get that $29^{\phi(13)} \equiv 1(\text{mod}13)$.

Since 13 is prime, it follows that $\phi(13)=12$, hence $29^{12} \equiv 1(\text{mod}13)$.

We can now apply the division algorithm between 202 and 12 as follows:

$$202=12(16)+10$$

Hence it follows that $29^{202}=(29^{12})^{26} \cdot 29^{10} \equiv (1)^{26} \cdot 29^{10} \equiv 29^{10}(\text{mod}13)$.

Also we note that 29 can be reduced to 3 (mod 13), and hence:

$$29^{10} \equiv 3^{10}=59049 \equiv 3(\text{mod}13)^2$$

Hence when 29^{202} is divided by 13, the remainder leftover is 3.

Example: Find the remainder of 99^{999999} when divided by 23.
Solution: Once again we note that (99,23)=1, hence it follows that $99^{\phi(23)} \equiv 1(\text{mod}23)$.

Once again, since 23 is prime, it goes that $\phi(23)=22$, and more appropriately 9922≡1(mod23).

We will now use the division algorithm between 999999 and 22 to get that:

$$999999=22(45454)+11$$

Hence it follows that
$99^{999999}=(99^{22})^{45454} \cdot 99^{11} \equiv 1^{45454} \cdot 99^{11} \equiv 7^{11}=1977326743 \equiv 22(\text{mod}23)$.

Hence the remainder of 99^{999999} when divided by 23 is 22.

Note that we can solve the final congruence a little differently as:
$99^{1}1 \equiv 7^{11}=(7^{2})^{5} \cdot 7=(49)^{5} \cdot 7 \equiv 3^{5} \cdot 7=1701 \equiv 22(\text{mod}23)$.

There are many ways to evaluate these sort of congruences, some easier than others.

Example: What is the remainder when 13^{18} is divided by 19?
Solution: If $y^{\phi\,(z)}$ is divided by z, the remainder will always be 1; if y, z are co-prime
In this case the Euler number of 19 is 18

(The Euler number of a prime number is always 1 less than the number).

As 13 and 19 are co-prime to each other, the remainder will be 1.

Example: Now, let us solve the question given at the beginning of the article using the concept of Euler Number: What is the remainder of $19^{2200002}/23$?

Solution: The Euler Number of the divisor i.e. 23 is 22, where 19 and 23 are co-prime.

Hence, the remainder will be 1 for any power which is of the form of 220000.
The given power is 2200002.
Dividing that power by 22, the remaining power will be 2.
Your job remains to find the remainder of $19^2/23$.
As you know the square of 19, just divide 361 by 23 and get the remainder as 16.

Example: Find the last digit of 55^5.

Sol: We first note that finding the last digit of 55^5 can be obtained by reducing 55^5 (mod 10), that is evaluating 55^5(mod10).

We note that (10, 55) = 5, and hence this pair is not relatively prime,
however, we know that 55 has a prime power decomposition of
55 = 5 x 11. (11, 10) = 1,
hence it follows that $11^{\phi(10)} \equiv 1 \pmod{10}$.
We note that $\phi(10)=4$. Hence $11^4 \equiv 1 \pmod{10}$, and more appropriately:
$55^5=5^5\cdot 11^5=5^5\cdot 11^4\cdot 11\equiv 5^{12}\cdot(1)^4\cdot 11\equiv 34375\equiv 5 \pmod{10}$
Hence the last digit of 55^5 is 5.

Example: Find the last two digits of 3333^{4444}.

Sol:

We first note that finding the last two digits of 3333^{4444} can be obtained by reducing 3333^{4444} (mod 100).
Since (3333, 100) = 1, we can apply this theorem.
We first calculate that $\phi(100)=\phi(2^2)\phi(5^2)=(2)(5)(4)=40$.
Hence it follows from Euler's theorem that $3333^{40}\equiv 1 \pmod{100}$.
Now let's apply the division algorithm on 4444 and 40 as follows:

$$4444=40(111)+4$$

Hence it follows that:
$3333^{4444}\equiv(3333^{40})^{111}\cdot 3333^4\equiv(1)^{111}\cdot 3333^4 \pmod{100}\equiv 33^4=1185921\equiv 21 \pmod{100}$
Hence the last two digits of 3333^{4444} are 2 and 1.

Previous questions

1. a) Prove that a group consisting of three elements is an abelian group?
   b) Prove that G={-1,1,i,-i} is an abelian group under multiplication?
2. a) Let G= {-1,0,1} . Verify that G forms an abelian group under addition?
   b) Prove that the Cancellation laws holds good in a group G.?
3. Prove that the order of a^{-1} is same as the order of a.?
4. a) Explain in brief about fermats theorem?
   b) Explain in brief about Division theorem?
   c) Explain in brief about GCD with example?
5. Explain in brief about Euler's theorem with examples?
6. Explain in brief about Principle of Mathematical Induction with examples?
7. Define Prime number? Explain in brief about the procedure for testing of prime numbers?
8. Prove that the sum of two odd integers is an even integer?
9. State Division algorithm and apply it for a dividend of 170 and divisor of 11.
10. Using Fermat's theorem, find 3^{201} mod 11.
11. Use Euler's theorem to find a number between 0 and 9 such that *a* is congruent to 7^{1000} (mod 10)
12. Find the integers x such that i) 5x≡4 (mod 3) ii) 7x≡6 (mod 5) iii) 9x≡8 (mod 7)
13. Determine GCD (1970, 1066) using Euclidean algorithm.
14. If a=1820 and b=231, find GCD (a, b). Express GCD as a linear combination of a and b.
15. Find 11^7 mod 13 using modular arithmetic.

Multiple choice questions

1. If a|b and b|c, then a|c.
   a) True b) False
   Answer: a
2. GCD(a,b) is the same as GCD(|a|,|b|).
   a) True b) False
   Answer: a
3. Calculate the GCD of 1160718174 and 316258250 using Euclidean algorithm.
   a) 882 b) 770 c) 1078 d) 1225
   Answer: c
4. Calculate the GCD of 102947526 and 239821932 using Euclidean algorithm.
   a) 11 b) 12 c) 8 d) 6
   Answer: d
5. Calculate the GCD of 8376238 and 1921023 using Euclidean algorithm.
   a) 13 b) 12 c) 17 d) 7
   Answer: a
6. What is 11 mod 7 and -11 mod 7?
   a) 4 and 5 b) 4 and 4 c) 5 and 3 d) 4 and -4
   Answer: d
7. Which of the following is a valid property for concurrency?
   a) a = b (mod n) if n|(a-b) b) a = b (mod n) implies b = a (mod n)
   c) a = b (mod n) and b = c (mod n) implies a = c (mod n)
   d) All of the mentioned
   Answer: d
8. [(a mod n) + (b mod n)] mod n = (a+b) mod n
   a) True b) False
9. [(a mod n) – (b mod n)] mod n = (b – a) mod n
   a) True b) False
   Answer:b

10. 11^7 mod 13 =
a) 3 b) 7 c) 5 d) 15
Answer: d
11. The multiplicative Inverse of 1234 mod 4321 is
a) 3239 b) 3213 c) 3242 d) Does not exist
Answer: a
12. The multiplicative Inverse of 550 mod 1769 is
a) 434 b) 224 c) 550 d) Does not exist
Answer: a
13. The multiplicative Inverse of 24140 mod 40902 is
a) 2355 b) 5343 c) 3534 d) Does not exist
Answer: d
14. GCD(a,b) = GCD(b,a mod b)
a) True b) False
Answer: a
15. Define an equivalence relation R on the positive integers A = {2, 3, 4, . . . , 20} by m R n if the largest prime divisor of m is the same as the largest prime divisor of n. The number of equivalence classes of R is
(a) 8 (b) 10 (c) 9 (d) 11 (e) 7
Ans:a
16. The set of all nth roots of unity under multiplication of complex numbers form a/an
A.semi group with identity B.commutative semigroups with identity
C.group D.abelian group
Option: D
17. Which of the following statements is FALSE ?
A.The set of rational numbers is an abelian group under addition
B.The set of rational integers is an abelian group under addition
C.The set of rational numbers form an abelian group under multiplication
D.None of these
Option: D
18.In the group G = {2, 4, 6, 8) under multiplication modulo 10, the identity element is
A.6 B.8 C.4 D.2
Option: A
19. Match the following
A. Groups I. Associativity
B. Semi groups II. Identity
C. Monoids III. Commutative
D. Abelian Groups IV Left inverse

A.	A	B	C	D	B.	A	B	C	D	C.	A	B	C	D	D.	A B C D
	IV	I	II	III		III	I	IV	II		II	III	I	IV		I II III IV

Option: A
20. Let (Z,*) be an algebraic structure, where Z is the set of integers and the operation * is defined by n*m = maximum(n,m). Which of the following statements is TRUE for (Z,*)?
A.(Z, *) is a monoid B.(Z, *) is an abelian group C.(Z, *) is a group D.None
Option: D
21. Some group (G,0) is known to be abelian. Then which of the following is TRUE for G ?
A.$g = g^{-1}$ for every $g \in G$ B.$g = g^2$ for every $g \in G$
C.$(g \text{ o } h)^2 = g^2 \text{o } h^2$ for every $g,h \in G$ D.G is of finite order
Option: C
22. If the binary operation * is deined on a set of ordered pairs of real numbers as (a, b)*(c, d)

= (ad + bc, bd) and is associative, then (1, 2) * (3, 5) * (3, 4) equals

A.(74,40) B.(32,40) C.(23,11) D.(7,11)

Option: A

23. The linear combination of gcd(252, 198) = 18 is

a) 252*4 – 198*5 b) 252*5 – 198*4 c) 252*5 – 198*2 d) 252*4 – 198*4

Answer:a

24. The inverse of 3 modulo 7 is

a) -1 b) -2 c) -3 d) -4

Answer:b

25. The integer 561 is a Carmichael number.

a) True b) False

Answer:a

26. The linear combination of gcd(117, 213) = 3 can be written as

a) 11*213 + (-20)*117 b) 10*213 + (-20)*117

c) 11*117 + (-20)*213 d) 20*213 + (-25)*117

Answer:a

27. The inverse of 7 modulo 26 is

a) 12 b) 14 c) 15 d) 20

Answer:c

28. The inverse of 19 modulo 141 is

a) 50 b) 51 c) 54 d) 52

Answer:d

29. The value of 5^{2003} mod 7 is

a) 3 b) 4 c) 8 d) 9

Answer:a

30. The solution of the linear congruence 4x = 5(mod 9) is

a) 6(mod 9) b) 8(mod 9) c) 9(mod 9) d) 10(mod 9)

Answer:b

31. The linear combination of gcd(10 ,11) = 1 can be written as

a) (-1)*10 + 1*11 b) (-2)*10 + 2*11

c) 1*10 + (-1)*11 d) (-1)*10 + 2*11

Answer:a