Combinatorics

Permutation :-

An ordered arrangement of r elements of a set containing n distinct elements is called an r-permutation of n elements and is denoted by $P(n,r)$ or ${}^nP_r$, where $r \leq n$.

Combinations :-

An unordered selection of r elements of a set containing n distinct elements is called an r-combination of n elements and is denoted by $C(n,r)$ or ${}^nC_r$ or $\binom{n}{r}$.

Note :- A permutation of objects involves ordering whereas a combination does not take ordering into account

Values of $P(n,r)$

The first elt of the permutation can be selected from a set having n elements in n ways The second element can be selected in $(n-1)$ ways as there are $(n-1)$ elts left in the set. Similarly there are $(n-2)$ ways for selecting the 3rd elt and so, on. Finally there are $n-(r-1) = n-r+1$ ways of selecting the r^{th} element.

Consequently, there are

$n(n-1)(n-2)\cdots(n-r+1)$ ways of

ordered arrangement of r elements of the given set.

Thus $P(n,r) = n(n-1)(n-2)\cdots(n-r+1)$

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

In particular $\boxed{P(n,n) = n!}$

Product Rule:-

If an activity can be performed in r successive steps and step 1 can be done in n_1 ways, step 2 can be done in n_2 ways ... step r can be done in n_r ways, then the activity can be done in

$(n_1 \times n_2 \times \cdots \times n_r)$ ways.

Also $P(n,r) = C(n,r) \cdot P(r,r)$

(first forming the $C(n,r)$ r-combinations of the set and then arranging (ordering) the elts in each r-combinations, which can be done in $P(r,r)$ ways)

Thus $C(n,r) = \dfrac{P(n,r)}{P(r,r)} = \dfrac{n!}{(n-r)!} \dfrac{(r-r)!}{r!}$

$$\Rightarrow \boxed{C(n,r) = \frac{n!}{r!\,(n-r)!}}$$

In particular $\boxed{C(n,n) = 1}$

Note:- Since the number of ways of selecting out r elements from a set on n elements is the same as the number of ways of leaving $(n-r)$ elements in the set, it follows that

$$\boxed{C(n,r) = C(n, n-r)}$$

Otherwise

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

$$= C(n,r)$$

Sum rule:-

If r activities can be performed in $n_1, n_2 \cdots n_r$ ways and if they are disjoint, viz, cannot be performed simultaneously, then any one of the r activities can be performed in $(n_1 + n_2 + \cdots + n_r)$ ways.

Permutations with repetition:-

Theorem:- When repetition of n elements contained in a set is permitted in r-permutations, then the number of r-permutations is n^r.

Theorem:- The number of different permutations of n objects which include n_1 identical objects of type I, n_2 identical objects of type II, ... and n_k identical objects

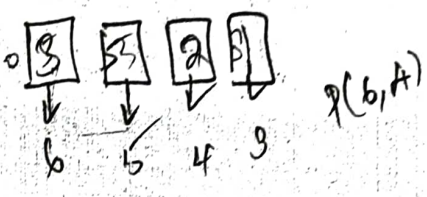
of type k is equal to $\frac{n!}{n_1!\, n_2! \cdots n_k!}$, where

$n_1 + n_2 + \cdots + n_k = n$

Circular Permutation:-

The no. of different circular arrangements of n objects $= (n-1)!$

If no distinction is made between clockwise and counter clockwise circular arrangements, then the no. of different circular arrangements $= \frac{1}{2}(n-1)!$



Problems:-

1 (a) Assuming that repititions are not permitted, how many 4-digit nos can be formed from the six digits 1, 2, 3, 5, 7, 8?

the 4-digit no. can be considered to be formed by filling up 4 blank spaces with the available 6 digits. Hence the no. of 4-digit nos

= number of 4-permutations of 6 nos

= $P(6;4) = 6 \times 5 \times 4 \times 3 = 360$

(b) How many of these nos are less than 4000?

If a 4-digit nos. is to be less than 4000, the first digit must be 1, 2 or 3. Hence the first space can be filled up in 3 ways. Corresponding to any of these 3 ways, the remaining 3 spaces can be filled up with the remaining 5 digits in $P(5,3)$ ways. Hence the required number

= $3 \times P(5,3)$ ways

= $3 \times (5 \times 4 \times 3) = 180$

(c) How many of these nos. in part (a) are even?

If the 4-digit no. is to be even, the last digit must be 2 or 8. Hence the last space can be filled up in 2 ways. Corresponding to any one of these 2 ways, the remaining 3 spaces can be filled up with the remaining

$P(5,3) \times 2$

5 digits in $P(5,3)$ ways. Hence the required

no. of even nos $= 2 \times P(5,3) = 2 \times (5 \times 4 \times 3) = 120$

(d) How many of the nos in part (a) are odd?

Odd digits 1, 3, 5, 7 _ _ _ _ 1 or 3 or 5 ⇒ (3 ways)

No of ways $= 4 \times P(5,3) = 240$

(e) How many of the nos in part (a) are multiples of 5?

Last digit has to be 5 for multiple of 5

So only one way of filling it. Rem places $P(5,3)$

No of ways $= 1 \times P(5,3) = 60$

f) How many of the nos in part (a) contain both the digits 3 and 5.

The digits 3 and 5 can occupy any 2 of the 4 places in $P(4,2) = 4 \times 3 = 12$ ways.

The remaining 2 places can be filled by the remaining 4 digits in $P(4,2)$ ways.

So the required no. of ways $= 12 \times 12 = 144$.

- The no. of arrangements of all the six letters in the word PEPPER?

no. of arrangements $= \frac{6!}{3!\,2!} = \frac{720}{6(2)} = 60$

$\square\ \square\ \square\ \square$ (3!)

$P(4,2) \times P(4,2)$ $\quad \frac{6!}{3!\,2!}$

(2)(a) In how many ways can 6 boys and 4 girls sit in a row?

6 boys and 4 girls ⇒ totally 10 persons can sit in a row (ie arranged in 10 places) in $P(10,10) = 10!$ ways

(b) In how many ways can they sit in a row if the boys are to sit together and the girls are to sit together?

bbbbbb gggg
gggg bbbbbb } – 2 ways

Let us assume that the boys are combined as one unit and the girls are combined as another unit. These 2 units can be arranged in $2!$ ways $= 2$ ways.

Corresponding to one of the 2 ways, the boys can be arranged in a row in $6!$ ways and the girls in $4!$ ways.

∴ Required no. of ways $= 2! \times 6! \times 4! = 34,560$

(c) In how many ways can they sit in a row if the girls are to sit together?

The girls are considered as one unit (object) and there are 7 objects consisting of one object of 4 girls and 6 objects of 6 boys.

These 7 objects can be arranged in a row in $7!$ ways corresponding to one of these ways, the 4 girls (considered as one object) can be arranged

among themselves in 4! ways.

∴ Required no of ways = 7! × 4! = 1,20,960

(X) B G B G B G B G B G B (X)

d) In how many ways can they sit in a row if just the girls are to sit together?

7! × 4!

No. of ways in which girls only sit together
= (No of ways in which girls sit together)
— (No. of ways in which boys sit together and girls sit together)

= 1,20,960 − 34,560 = 86,400.

bb 9999 bbbb
bbb 9999 bb

3. How many positive integers n can be formed using the digits 3,4,4,5,5,6,7 if n has to exceed 50,00,000?

Ans In order that n may be greater than 50,000, the first place must be occupied by 5, 6 or 7.

When 5 occupies the first place, the remaining 6 places are to be occupied by the digits 3,4,4,5,6,7.

The number of such numbers

$$= \frac{6!}{2!}$$ (because the digit 4 occurs twice)

= 360.

When 6 occupies the first place the remaining 6 places can be occupied by the digits 3,4,4,5,5,7 ⇒ No of such nos = $\frac{6!}{2!\,2!}$

(4 & 5 occurs twice) = 180

IIIly for 7 we have other nos as 3,4,4,5,56

No of such nos $= \frac{6!}{2!\,2!} = 180$.

So, the no. of numbers exceeding 50,00,000

$= 360 + 180 + 180 = 720$

(A) (a) If 6 people A, B, C, D, E, F are seated about a round table, how many different circular arrangements are possible, if arrangements are considered the same when one can be obtained from the other by rotation?

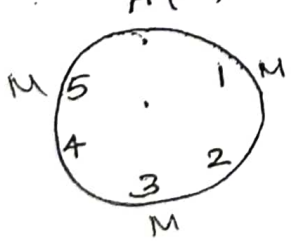
The no. of different circular arrangements of n objects is $(n-1)!$

∴ The required no. of circular arrangements

$= 5! = 120$.

(b) If A, B, C are females and the others are males, in how many arrangements do the sexes alternate?

Soln:- Since rotation does not alter the circular arrangement, we can assume that A occupies the top position as shown in the figure



Of the remaining places, position 1, 3, 5 must be occupied by the 3 males. This can be achieved by $P(3,3) = 3! = 6$ ways.

The remaining two places 2 and 4 should be occupied by the remaining two females. This can be achieved in $P(2,2)$

$= 2! = 2$ ways.

$\therefore$ Total no. of required circular arrangements

$= 6 \times 2 = 12$ ways.

5. From a club consisting of 6 men and 7 women, in how many ways can we select a committee of

(a) 3 men & 4 women.

3 men can be selected from 6 men in $C(6,3)$ ways & 4 women can be selected from 7 women in $C(7,4)$ ways.

$\therefore$ 3 m & 4 W $= C(6,3) \times C(7,4)$ ⟶ (By Product Rule)

$= \frac{6!}{3!\,3!} \times \frac{7!}{4!\,3!} = 700$ ways.

(b) 4 person which has atleast one women

Atleast 1 W ⇒ 1W + 3M $\quad C(7,1) \cdot C(6,3)$

(or) 2W ⇒ 2W + 2M $\quad C(7,2) \cdot C(6,2)$

(or) 3W ⇒ 3W + 1M $\quad C(7,3) \cdot C(6,1)$

(or) 4W ⇒ 4W + 0M $\quad C(7,4) \cdot C(6,0)$

Total no. of ways $C(7,1)C(6,3) + C(7,2)C(6,2) + C(7,3) \cdot C(6,1) + C(7,4) \cdot C(6,0)$

$= 20 \times 7 + 15 \times 21 + 6 \times 35 + 1 \times 35 = 700$ ways.

$= 140 + 315 + 210 + 35$

(c) 4 person that has atmost one man.

⇒ 1 m + 3 w (or) 0 m + 4 w

$= C(6,1) \cdot C(7,3) + C(6,0) \cdot C(7,4)$

$= 1 \times 35 + 6 \times 35 = 245$ ways

(d) 4 persons that has persons of both sexes C

3W & 1M (or) 2W & 2M (or) 1W & 3M

$= C(6,1) \cdot C(7,3) + C(6,2) \cdot C(7,2) + C(6,3) \cdot C(7,1)$

$= 6 \times 35 + 15 \times 21 + 20 \times 7 = 210 + 315 + 140 = 665$

Principle of Inclusion - Exclusion

Statement:-

If A & B are finite subsets of a finite universal set U, then

$|A \cup B| = |A| + |B| - |A \cap B|$, where $|A|$ denotes the cardinality of (the no. of elts) the sets A

The Principle can be extended to a finite number of finite sets $A_1, A_2, \ldots A_n$ as follows,

$$|A_1 \cup A_2 \cup \ldots \cup A_n| = \sum_i |A_i| - \sum_{i<j} |A_i \cap A_j| + \sum_{i<j<k} |A_i \cap A_j \cap A_k| - \ldots + (-1)^{n+1} |A_1 \cap A_2 \cap \ldots \cap A_n|$$

Problem: There are 250 students in an engineering college. Of these 188 have taken a course in Fortran, 100, have taken a course in C and 35 have taken a course in Java. Further 88 have taken courses in both Fortran and C. 23 have taken courses in both C and Java. 29 have taken courses in both Fortran and Java. If 19 of these students have taken all the 3 courses, how many of these 250 students have not taken a course in any of these 3 programming language?

Soln: Let F, C, J denote the students who have taken the languages Fortran, C & Java resp/.

Then $|F| = 188$; $|C| = 100$; $|J| = 35$

$|F \cap C| = 88$; $|C \cap J| = 23$; $|F \cap J| = 29$

and $|F \cap C \cap J| = 19$.

Then the no. of students who have taken atlea one of the three languages is given by

$$|F \cup C \cup J| = |F| + |C| + |J| - |F \cap C| - |F \cap J| - |C \cap J| + |F \cap C \cap J|$$

$$= (188 + 100 + 35) - 88 - 29 - 23 + (19)$$

$$= 323 - 140 + 19 = 202.$$

∴ No. of students who have not taken a course in any of these languages $= 250 - 202 = \underline{\underline{48}}$

2i. Find the no. of integers between 1 and 250 both inclusive that are not divisible by any of the integers 2, 3, 5 and 7.

Let A, B, C, D be the sets of integers that lie between 1 and 250 and that are divisible by 2, 3, 5 and 7 respectively.

The elements of A are 2, 4, 6 ... 250

$|A| = \lfloor \frac{250}{2} \rfloor = 125$ $|D| = \lfloor \frac{250}{7} \rfloor = 35$.

$|B| = \lfloor \frac{250}{3} \rfloor = 83$

$|C| = \lfloor \frac{250}{5} \rfloor = 50$

(eg) 1 – 10

A = divisible by 2 = 2, 4, 6, 8, 10

$|A| = \lfloor \frac{10}{2} \rfloor = 5$

B = divisible by 3 = 3, 6, 9

$B = \lfloor \frac{10}{3} \rfloor = \lfloor 3.33 \rfloor = 3$

$C = \lfloor \frac{10}{5} \rfloor = 2$ (5, 10)

$D = \lfloor \frac{10}{7} \rfloor = 1$ (7)

During a four week vacation, a school student will attend at least one computer class each day, but he won't attend more than 40 classes in all during the vacation. Proove that, no matter how he distributes his classes during the four weeks, there is a consecutive span of days during which he will attend exactly 15 classes.

Soln: Let a_i = no. of classes the student attends on day i

b_i = no. of classes the student attends on or before day i

Then $b_i = a_1 + a_2 + \cdots + a_i$ – cummulative classes attended till day i

~~From day 1 the~~ He totally has to attend 40 classes

So $1 \le b_1 < b_2 < b_3 \cdots < b_{28} \le 40$

and $15 \le (b_1+15) < (b_2+15) < \cdots < (b_{28}+15) \le 55$

$(b_1, b_2, \ldots, b_{28})$ → different 28 integers

$(b_1+15, b_2+15, \ldots, b_{28}+15)$ → " " "

Total ≤ 56 distinct integers

But total 55 different values. So by Pigeon hole principle, atleast 2 of the 56 numbers are equal

Since $b_j > b_i$ if $j > i$, the only possible way for 2 nos to be equal is $b_j = b_i + 15$ (for some i, j with $j > i$)

$\Rightarrow b_j - b_i = 15$

(i.e) $a_{i+1} + a_{i+2} + \cdots + a_j = 15$

(i.e) from the start of day $(i+1)$ to the end of day j, the student will attend exactly 15 classes

Pigeonhole Principle :-

Statement :- If n pigeons are accommodated in m pigeon holes and $n > m$ then at least one pigeonhole will contain two or more pigeons. Equivalently, if n objects are put in m boxes and $n > m$, then at least one box will contain two or more objects.

Generalisation of the pigeonhole principle

If n pigeons are accomodated in m pigeon holes and $n > m$ then one of the pigeonholes must contain at least $\left\lfloor \frac{(n-1)}{m} \right\rfloor + 1$ pigeons, where $\lfloor x \rfloor$ denotes the greatest integer less than or equal to x, which is a real number

Q.1. A man hiked for 10 hrs and covered a total distance of 45 km. It is known that he hiked 6 km in the 1st hr and only 3 km in the last hour, Show that he must have hiked atleast 9 km within a certain period of two consecutive hrs.

Soln: Since the man hiked $6+3 = 9$ km in the first last hrs, he must have hiked $45-9 = 36$ kms during the period from second to ninth hr.

If we combine the 2nd & 3rd hrs together, the 4th & 5th hr together, etc. the 8th & 9th hrs together, we have 4 time periods Let us now treat 4 time periods as pigeonholes and 36 kms as 36 pigeons. Using generalised pigeonhole principal, the least no. of pigeons accomodated in one pigeonhole

$$= \left\lfloor \frac{36-1}{4} \right\rfloor + 1 = \lfloor 8.75 \rfloor + 1 = 9$$

(or) the man must have hiked atleast 9km in one time period of 2 consecutive hrs.

2. Prove that in any group of 6 ppl, at least 3 must be friends or atleast 3 must be mutual strangers.

Let A be one of the six people. Let the remaining 5 ppl be accomodated in 2 rooms labeled 'A's friends' and 'strangers to A'. Treating 5 ppl as 5 pigeons and 2 rooms as pigeonholes, by the generalised pigeonhole principle, one of the rooms must contain $\left\lfloor \frac{5-1}{2} \right\rfloor + 1 = 3$ people

Let the room labeled 'A's friends' contain 3 ppl. If any 2 of these 3 ppl are friends, then together with A, we have a set of 3 mutal friends. If no two of these 3 ppl are friends, then these 3 ppl are mutual strangers. In either cases, we get the required conclusion. If the room labeled 'strangers to A' contain 3 ppl, we get the required conclusion by similar argument.

4. If 9 colours are used to paint 100 houses, show that atleast 12 houses will be of the same colour

$$\left\lfloor \frac{100-1}{9} \right\rfloor + 1 = 12$$

5. In a grp of 100 ppl, several will have birthdays in the same month. Atleast how many must have birth days in the same month?

$$\left\lfloor \frac{100-1}{12} \right\rfloor + 1 = \lfloor 8.25 \rfloor + 1 = 9$$ (so out of 100 ppl were born in the

6. Sh in a grp of 8 ppl, atleast 2 have birthdays which fall on the same day of the weak in any given weak.

7. What is the minimum number of students required in a class to be sure that atleast six will receive the same grade, if there are 5 possible grades?

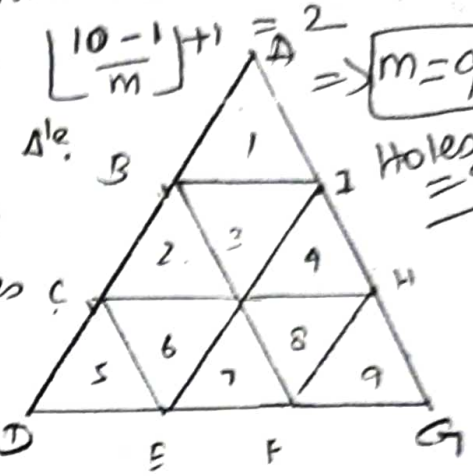
11. If we select 10 points in the interior of an equilateral triangle of side 1, show that there must be atleast 2 pts whose distance apart is less than $\frac{1}{3}$

$\left\lfloor \frac{10-1}{m} \right\rfloor + 1 = 2 \Rightarrow m = 9$

Holes = 9

Soln: Let ADG be the given equilateral Δ^{le}.

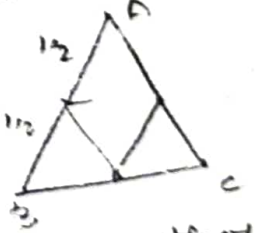
The pairs of points B, C ; E, F and H, I are the points of trisection of the sides AD, DG and GA resp. We have divided the Δ^{le} ADG into 9 equilateral Δ^{le}s each of side 1/3.



The 9 sub triangles may be regarded as 9 pigeon ~~pegeo~~ holes and 10 interior pts may be regarded as 10 ~~interior~~ pts. Then by the pigeonhole principle, atleast one sub Δ^{le} must contain 2 interior pts. The distance between any two interior points of any sub Δ^{le} cannot exceed the length of the side, namely 1/3. Hence the proof.

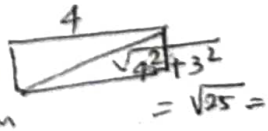
12. If there are 5 points inside a square of side length 2, prove that two of the points are within a distance of $\sqrt{2}$ of each other.

13. Of any 5 pts chosen within an equilateral Δ^{le} whose sides are of length 1, show that 2 are within a distance of $\frac{1}{2}$ of each other



14. Of any 26 points within a rectangle measuring 20 cm by 15 cm, show that atleast two are within 5 cm of each other

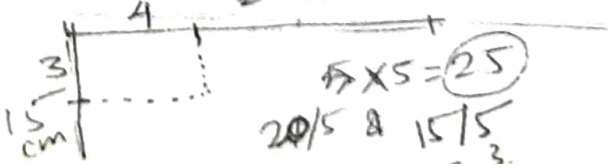
Divide 20×15 into 25 rectangles of side 4×3 each.



$\left\lfloor \frac{26-1}{m} \right\rfloor + 1 = 2$

$\frac{25}{m} = 1 \Rightarrow 25 = m$

holes = 25



Sol'n Let n be the smallest such integer such that

$$\left\lfloor \frac{n-1}{5} \right\rfloor + 1 = 6 \Rightarrow \left\lfloor \frac{n-1}{5} \right\rfloor = 5 \Rightarrow n-1 = 25 \quad \boxed{n=}$$

8. What is the minimum number of students, each of whom comes from one of the 50 states, who must be enrolled in a university to guarantee that there are atleast 100 who come from the same state?

$$\left\lfloor \frac{n-1}{50} \right\rfloor + 1 = 100 \Rightarrow \left\lfloor \frac{n-1}{50} \right\rfloor = 99 \Rightarrow n-1 = 99(50)$$

$$n = 4950+1 = 4951$$

9. Among any grp of 367 ppl, there must be atleast 2 with the same birthday, because there are only 366 possible birthdays

10. In a grp of 27 English words, there must be atleast 2 that begin with the same letter, because there are 26 letters in the English alphabet.

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

The set of integers between 1 and 250 which are divisible by 2 and 3 i.e. $A \cap B$ is the same as that which is divisible by 6, since 2 and 3 are relatively prime nos. $2 \times 3 = 6$

$\therefore |A \cap B| = \left\lfloor \frac{250}{6} \right\rfloor = 41$

$|A \cap C| = \left\lfloor \frac{250}{10} \right\rfloor = 25$ ($5 \times 2 = 10$)

$|C \cap D| = \left\lfloor \frac{250}{35} \right\rfloor = 7$ ($7 \times 5 = 35$)

$|A \cap B \cap C| = \left\lfloor \frac{250}{30} \right\rfloor = 8$ ($2 \times 3 \times 5 = 30$)

$|A \cap C \cap D| = \left\lfloor \frac{250}{70} \right\rfloor = 3$ ($2 \times 5 \times 7 = 70$)

$|A \cap B \cap C \cap D| = \left\lfloor \frac{250}{210} \right\rfloor = 1$.

$|A \cap D| = \left\lfloor \frac{250}{14} \right\rfloor = 17$ ($7 \times 2 = 14$)

$|B \cap D| = \left\lfloor \frac{250}{21} \right\rfloor = 11$ ($7 \times 3 = 21$)

$|B \cap C| = \left\lfloor \frac{250}{15} \right\rfloor = 16$ ($5 \times 3 = 15$)

$|A \cap B \cap D| = \left\lfloor \frac{250}{42} \right\rfloor = 5$ ($2 \times 3 \times 7 = 42$)

$|B \cap C \cap D| = \left\lfloor \frac{250}{105} \right\rfloor = 2$ ($3 \times 5 \times 7 = 105$)

By the principle of Inclusion–Exclusion, the number of integers between 1 – 250 that are divisible by at least one of 2, 3, 5 and 7 is

$|A \cup B \cup C \cup D| = \{|A| + |B| + |C| + |D|\} - \{|A \cap B| + |B \cap C| + \dots |C \cap D|\} + \{|A \cap B \cap C| \dots |B \cap C \cap D|\} - \{|A \cap B \cap C \cap D|\}$

$= (125 + 83 + 50 + 35) - (41 + 25 + 17 + 16 + 11 + 7) + (8 + 5 + 3 + 2) - 1 = 293 - 117 + 18 - 1 = 193$

∴ Number of integers between 1 and 250 that are not divisible by any of the integers 2, 3, 5 and 7.

= Total no. of integers − $|A \cup B \cup C \cup D|$

= 250 − 193 = 57.

5. Using prime factorisation, find the gcd and lcm of (i) (231, 1575)

$231 = 3^1 \cdot 7^1 \cdot 11^1 \cdot 5^0$

$1575 = 3^2 \cdot 7^1 \cdot 5^2 \cdot 11^0$

3 | 231
7 | 77
11

3 | 1575
5 | 525
3 | 105
7 | 35
5

$\gcd(231, 1575) = 3^{\min(1,2)} \cdot 5^{\min(0,2)} \cdot 7^{\min(1,1)} \cdot 11^{\min(1,0)}$

$= 3^1 \cdot 5^0 \cdot 7^1 \cdot 11^0$

$= 3 \times 7 = 21$

$\text{lcm}(231, 1575) = 3^{\max(1,2)} \cdot 5^{\max(0,2)} \cdot 7^{\max(1,1)} \cdot 11^{\max(1,0)}$

$= 3^2 \cdot 5^2 \cdot 7^1 \cdot 11^1 = 9 \times 25 \times 7 \times 11$

$= 17325.$

Verification:- $\gcd(a,b) \times \text{lcm}(a,b) = ab$

$21 \times 17325 = 231 \times 1575$

$363825 = 363825$

Hence Verified.

6. Prime factorization of 6647

Begin with 2. None of the primes 2, 3, 5, 7, 11 and 13 divides 6647. But 17 divides 6647

17 | 6647
17 | 391
23

$\Rightarrow 6647 = 17^2 \cdot 23.$

7. If $\gcd(a,b) = 1$, prove that

$\gcd(2a+b, a+2b) = 1$ or 3

Soln Let $\gcd(2a+b, a+2b) = d$

Since d is a divisor of $2a+b$, we've

$$2a+b = k_1 d \quad - (1)$$

Nly $\quad a+2b = k_2 d \quad - (2)$

(1) − (2)

$$\begin{array}{rl} 4a + 2b &= 2k_1 d \\ (-)\ a + 2b &= k_2 d \\ \hline 3a \quad (-) & (-)\ (2k_1 - k_2)d \end{array}$$

$\Rightarrow 3a = (2k_1 - k_2)d \Rightarrow d$ divides $3a$

(2) − (1) $\Rightarrow 3b = (2k_2 - k_1)d \Rightarrow d$ divides $3b$

$\Rightarrow d \leq \gcd(3a, 3b) = 3\gcd(a,b)$ (property ③)

↓ divisor ↓ greatest common divisor

$\Rightarrow d \leq 3(1)$ as $\gcd(a,b) = 1$ (given)

$\Rightarrow d = 1$ or 2 or 3

When a is even b odd, $2a+b$ is odd & $a+2b$ is even

When a is odd b even, $2a+b$ is even & $a+2b$ is even

When both a & b are odd both $2a+b$ & $a+2b$ are odd

If Both a & b are even then $\gcd(\text{even}, \text{even}) \neq 1$

$\gcd(a,b) \neq 1$

which is a contradiction to the given fact that $\gcd(a,b) = 1$.

Hence both a & b cannot be even.
So d cannot be 2.
So only possibility for d is either 1 or 3.

8. If gcd (a,4) = gcd (b,4) = 2
prove that gcd (a+b, 4) = 4

Soln
When gcd (a,4) = 2, a is a multiple of 2 but not 4.
So $a = 2m$, for some odd integer m.
Similarly gcd (b,4) = 2 $\Rightarrow$ $b = 2n$, for some odd integer n.
Now $a+b = 2m+2n = 2(m+n)$
m → odd n → odd $\Rightarrow$ m+n is even.
so $2(m+n) = 2(2q)$ where q is an integer
∴ gcd (a+b, 4) = gcd (4q, 4) = 4.

9. Prove that cube of an integer has one of the forms $9k$, $9k+1$, $9k+8$.

Soln: By division algorithm, If b divides a then $a = bq + r$ where $0 \le r < b$

We have to prove cube of an integer has one of the forms $9k, 9k+1, 9k+8$

Comparing it with $a = bq + r$ we see that an integer 'a' is divided by 9. When it is divided by 9, then the possible remainder are $0 \le r < 9 \Rightarrow 0, 1, 2, 3, \ldots 8$.

So a will be of the form

$a = 9q$ (or) $9q+1$ (or) $9q+2$ (or) $\ldots$ (or) $9q+8$

When $a = 9q$ then $a^3 = (9q)^3 = 9(q^2q^3)$

which is of the form $9k$

When $a = 9q+1$ then $a^3 = (9q+1)^3$

$= 9^3q^3 + 3 \cdot 9^2 q + 3 \cdot 9 \cdot q^2 + 1$

$\Rightarrow$ form is $9k+1$ $= 9(9^2q^3 + 3 \cdot 9 \cdot q + 3 \cdot q^2) + 1$

$= 9k + 1$

When $a = 9q+2$ then $a^3 = (9q+2)^3$

$= 9^3q^3 + 3 \cdot 9^2 q + 3 \cdot 9 \cdot q^2 + 8 = 9(9^2q^2 + 3 \cdot 9 \cdot q + 3 \cdot q^2) + 8$

$\Rightarrow$ form is $9k+8$. $= 9k + 8$

Illy if we proceed $a = 9q+3$ is of form $9k$

$a = 9q+4 \Rightarrow 9k+1$, $a = 9q+5 \Rightarrow 9k+8$,

$a = 9q+6 \Rightarrow 9K$, $a = 9q+7 \Rightarrow 9K+1$, $a = 9q+8 \Rightarrow 9K+$

Thus, the cube of an integer is in any one of the form $9k$, $9k+1$ or $9k+8$.

10. If a is any positive integer, prove that $\gcd(a, a+2) = 1$ or 2.

Let $\gcd(a, a+2) = d$

$\Rightarrow a = K_1 d$

$a+2 = K_2 d$ $\Rightarrow 2 = (K_2 - K_1)d$ where $d \in$

If $K_2 - K_1 = 2$ then $d = 1$

or if $K_2 - K_1 = 1$ then $d = 2$

Hence the result.

11. If $\gcd(a,b) = 1$, then $\gcd(a^2, b^2) = 1$

Let $a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$ & $b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$

given $\gcd(a,b) = 1 \Rightarrow$ there is no common factor between a & b.

Prime factorisation of $a^2 = a \times a$

$= (p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n})(p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n})$

$= p_1^{a_1+a_1} p_2^{a_2+a_2} \cdots p_n^{a_n+a_n}$

$= p_1^{2a_1} p_2^{2a_2} \cdots p_n^{2a_n}$

III ly $b^2 = b \times b = p_1^{2b_1} p_2^{2b_2} \cdots p_n^{2b_n}$

They have no factor in common

Hence $\gcd(a^2, b^2) = 1$.

Number Theory

Deals with integers, more specifically positive integers & their property.

Applications in CSC → Transmission, coding and manipulation of numerical data & in Cryptology.

Divisibility :-

Defn:- When a and b are two integers with $a \neq 0$, a is said to divide b (ie a divides b or b is divisible by a) if there is an integer c such that $b = ac$ and it is denoted by the notation $a|b$

When a divides b, a is called a *divisor* or *factor* of b and b is called a *multiple* of a.

Note: When a divides b, then $-a$ also divides b since $b = ac$ can be rewritten as $b = (-a)(-c)$

Theorem:- Let $a, b, c \in \mathbb{Z}$, the set of integers. The

(i) If $a|b$ and $a|c$, then $a|(b+c)$

$a|b \Rightarrow b = ma$ m & n are integers

$a|c \Rightarrow c = na$

$b + c = (m+n)a \Rightarrow a|(b+c)$

(ii) If $a|b$ and $b|c$, then $a|c$.

$b = ma$ and $c = nb$; m & n are integers

$c = n(ma) = (nm)a \Rightarrow a|c$

(iii) If $a|b$, then $a|mb$, for any integer m.

Since $a|b \Rightarrow b = na$

$$mb = m(na) = (mn)a$$

(iv) If $a|b$ and $a|c$ then $a|(mb+nc)$ for any integers m & n

$a|b \Rightarrow a|mb$ (by iii)

$a|c \Rightarrow a|nc$ (by iii)

$a|mb$ and $a|nc \Rightarrow a|(mb+nc)$ (by i)

Prime Numbers

Defn:- A positive integer $p > 1$ is called prime, if the only positive factors of p are 1 and p.

A positive integer > 1 and is not prime is called Composite.

Note:(1) The positive integer 1 is neither prime nor composite.

(2) The positive integer n is composite, if there exists positive integers a and b such that $n = ab$ where $1 < a, b < n$.

Fundamental Theorem of Arithmetic

Every integer $n > 1$ can be written uniquely as a product of prime numbers.

Proof: By Induction.

Let $n = 2$.
Since 2 is prime, $(n = 2)$ is a product of primes (∵ a product may consist of a single factor)

Let $n > 2$.
If n is prime, it is a product of primes. (ie) a single factor product.
If n is not prime, (ie) composite, let us assume that the theorem holds good for positive integer less than n and that $n = ab$. Since $a, b < n$, each of a and b can be expressed as the product of primes (by the assumption).
∴ $n = ab$ is also a product of primes.

Note: (1) The unique expression for the integer $n > 1$ as a product of primes is called the prime factorisation or prime decomposition of n

$100 = 2^2 \cdot 5^2$; $5096 = 2^3 \cdot 7^2 \cdot 13$
$9999 = 9 \cdot 11 \cdot 101$

Theorem:- If $n > 1$ is a composite integer and p is a prime factor of n, then $p \leq \sqrt{n}$

Note: To test if a given integer n is prime, it is enough to see that it is not divisible by any prime less than or equal to $\sqrt{n}$.

(eg.) To check if 83 is prime, just chk $\sqrt{83} = 9.1\ldots$ prime less than 9, namely 2, 3, 5, 7. Since 83 is not divisible by any of these prime, 83 is prime.

Theorem:- The number of prime numbers is infinite.

Division Procedure.

Theorem:- When a and b are any two integers, $b>0$, there exist integers q and r such that $a = bq + r$, where $0 \le r < b$

Note:- ① The integers q and r are respectively called the quotient and the remainder when a is divisible by b

② When b is any integer, the above result can be stated as $a = qb + r$, where $0 \le r < |b|$

Example: If $a = 46$; $b = 13$ then $q = 3$ & $r = 7$

If $a = 46$, $b = -13 \Rightarrow q = -3$ and $r = 7$

If $a = -46$, $b = 13$ then $q = -4$ and $r = 6$

If $a = -46$, $b = -13$ then $q = 4$ and $r = 6$.

$b \overline{)a} \; q$; $0 \le r < b$

$13 \overline{)46} \; 3 = q$; -39 ; $7 = r$; $46 = 3 \times 13 + 7$

$-13 \overline{)46} \; -3 = q$; $+39$; $7 = r$; $46 = -3 \times -13 + 7$

$-13 \overline{)-46} \; 4$; $+52$; 6 ; $-46 = 4 \times -13 + 6$

$-13 \overline{)-46} \; 4$; -52 ; 6 ; $-46 = 4 \times 13 + 6 = -52 + 6 = -46$

Greatest Common Divisor

Defn:

When a and b are (non-zero) integers, then an integer $d(\neq 0)$ is said to be the common divisor of a and b, if $d|a$ and $d|b$ (ie d divides both a & b)

If d is the largest of all common divisors (ie. d is a multiple of every common divisor), then d is called the Greatest common divisor of a and b and denoted as $\gcd(a,b)$.

The greatest common divisor is also called the highest common factor for which the abbrevation is hcf (a,b).

If $\gcd(a,b) = 1$, then a and b are said to be relatively prime or) coprime or each is said to be prime to the other.

If $\gcd(a_i, a_j) = 1$ for $1 \le i < j \le n$, then the integers $a_1, a_2 \dots a_n$ are said to be pairwise relatively prime.

Eg: ① Let us consider the integers 9, 13, 25. Since $\gcd(9,13) = 1$, $\gcd(9,25) = 1$ and $\gcd(13,25) = 1$ so the integers 9, 13, 25 are pairwise relatively prime.

② Consider 10, 17, 25. $\gcd(10,17) = 1$, $\gcd(17,25) = 1$ and $\gcd(10,25) = 5$. Hence the integers 10, 17, 25 are not pairwise relatively prime

GCD of 24, 36

The common divisors are 1, 2, 3, 4, 6, 12

$\therefore \gcd(24,36) = 12$

$24 = 2^3 \times 3^1$

$36 = 2^2 \times 3^2$

$\therefore 2 \times 2 \times 2 \times 3 \quad 2 \times 2 \times 3 \times 3$

$2^3 \times 3^1, \quad 2^2 \cdot 3^2 \Rightarrow 2^{\min(3,2)} \times 3^{\min(1,2)}$

Euclid's Algorithm for finding gcd (a,b).

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).

Eg: find the gcd (1575, 231) by using Euclid's algorithm.

By division algorithm (quotient, remainder)

$$1575 = 6 \times 231 + 189 \Rightarrow$$
$$231 = 1 \times 189 + 42$$
$$189 = 4 \times 42 + 21$$
$$42 = 2 \times 21 + 0$$

Since the last non zero remainder is 21,

gcd (1575, 231) = 21.

231 | 1575 (6) , 1386 , 189

189 | 231 (1) , 189 , 42

42 | 189 (4) , 168 , 21

21 | 42 (2) , 42 , 0

Theorem:-

gcd (a,b) can be expressed as an integral linear combination of a and b.

(ie) gcd (a,b) = ma+nb, where m and n are integers.

Note: The expression of gcd (a,b) in the form ma+nb is not unique.

GCD (a,b) = GCD (b, a mod b)

if a>0 then b mod a = 0

Ex: GCD (10, 150) = GCD (10, 150 mod 10)

= GCD (10, 0)

GCD (10, 150) = 10.

150 => 15 × 10 + 0

10 | 150 (15) , 150 , 0

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

⑤ If $\gcd(a,b) = 1$, then for any integer c,
$\gcd(ac, b) = \gcd(c, b)$.

⑥ If each of $a_1, a_2, \cdots, a_n$ is coprime to b, then the product $(a_1 a_2 \cdots a_n)$ is also coprime to b

Least Common Multiple

Defn: 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 $\text{lcm}(a,b)$

Note: Even if both of a & b are negative, $\text{lcm}(a,b)$ is always positive (eg) $\text{lcm}(4,14) = \text{lcm}(-4,14)$
$= \text{lcm}(-4,-14) = 28$

Alternative defn. of $\text{lcm}(a,b)$:

If the prime factorisation of a & b are $a = p_1^{a_1} \cdot p_2^{a_2} \cdots p_n^{a_n}$ and $b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$, with conditions stated in the alternative defn. of $\gcd(a,b)$ then

$$\text{lcm}(a,b) = p_1^{\max(a_1,b_1)} \cdot p_2^{\max(a_2,b_2)} \cdots p_n^{\max(a_n,b_n)}$$

eg: $24 = 2^3 \cdot 3^1 \cdot 5^0$ and $30 = 2^1 \cdot 3^1 \cdot 5^1$

$$\text{lcm}(24,30) = 2^{\max(3,1)} \cdot 3^{\max(1,1)} \cdot 5^{\max(0,1)}$$
$$= 2^3 \cdot 3^1 \cdot 5^1 = 120$$

2	24, 30
3	12, 15
2	4, 5
	2, 5

$\text{lcm} = 2 \times 3 \times 2 \times 2 \times 5 = 120$

⑦ **Theorem:** If a and b are two positive integers, then $\boxed{\gcd(a,b) \cdot \text{lcm}(a,b) = ab}$

2	8
2	4
2	2
	1

2	32
2	16
2	8
2	4
2	2
	1

2	6
3	3
	1

2	4
2	2
	1

Eg:

8	12	6	4
16	12	12	8
24	24	18	12
32	36	24	16
40	48	30	20
48	60	36	24
56	72	42	28

$\therefore$ LCM = 24

Alternative definition of GCD (a, b)

If the prime factorisations of a and b are

$$a = p_1^{a_1} p_2^{a_2} p_3^{a_3} \cdots p_n^{a_n} \quad \text{and} \quad b = p_1^{b_1} p_2^{b_2} p_3^{b_3} \cdots p_n^{b_n}$$

where each exponent is a non-negative integer and where all primes occuring in the prime factorization of either a or b are included in both factorisations, with zero exponent if necessary, then

$$\gcd(a,b) = p_1^{\min(a_1,b_1)} \cdot p_2^{\min(a_2,b_2)} \cdots p_n^{\min(a_n,b_n)}$$

where $\min(x,y)$ means the minimum of the two numbers x and y.

$2 \mid 30$, $5 \mid 15$, 3 — $2 \mid 24$, $2 \mid 12$, $2 \mid 6$, 3

Eg:- $24 = 2^3 \cdot 3^1 \cdot 5^0$

$30 = 2^1 \cdot 3^1 \cdot 5^1$

$\therefore \gcd(24, 30) = 2^{\min(1,3)} \cdot 3^{\min(1,1)} \cdot 5^{\min(0,1)}$

$= 2^1 \cdot 3^1 \cdot 5^0 = 6.$

30: 1, 2, 3, 6 — 24: 1, 2, 3, 4, 6

Properties of GCD

① If $c \mid ab$ and a and c are coprime, then $c \mid b$

② If a and b are coprime and a and c are coprime, then a and bc are coprime.

~~③ If a and b are coprime and a and c are coprime, then a and bc are coprime.~~

③ If a, b are any integers, which are not simultaneously zero, and k is a positive integer, then $\gcd(ka, kb) = k \gcd(a, b)$.

Problems:

1) Find the prime factorization of the following.

a) $45,500 = 2^2 . 5^3 . 7^1 . 13^1$

2	45,500
2	22,750
5	11,375
5	2,275
5	455
7	91
	13

(b) $10! = 2.3.4.5.6.7.8.9.10$

$= 2\ 3.(2\times2)\ 5\ (2\times3)\ (7)\ (2\times2\times2)\ (3\times3)\ (5\times2)$

$= 2^8 . 3^4 . 5^2 . 7^1$

2. Prove that $\log_3 5$ is irrational

If possible let $\log_3 5 = \frac{r}{s}$ where r & s are positive int

$\Rightarrow 5 = 3^{r/s} \Rightarrow 3^r = 5^s = n$ say

Thus 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 of arithmetic. $\therefore \log_3 5$ is an irrational number

3. Use the Eulidean algorithm to find

(i) gcd (1819, 3587) and express the gcd as a linear combination of the given numbers.

Soln: By division algorithm

$3587 = 1 \times 1819 + 1768$ (1)

$1819 = 1 \times 1768 + 51$ (2)

for lcm

2	8, 12, 6, 4
2	4 6 3 2
2	2 3 3 1
3	1 3 3 1

$\Leftrightarrow 2\times2\times2\times3 = 24$

2	14, 14
2	2 7
7	1, 7
	1, 1

$= 2\times2\times7 = 28$

2	14 -14
2	-2 -7
7	-1 -7
	1 1

$$1768 = 34 \times 51 + 34 \quad (3)$$

$$51 = 1 \times 34 + 17 \quad (4)$$

$$34 = 2 \times 17 + 0.$$

Since the last non-zero remainder is 17, gcd (1819, 3587) = 17.

Now $17 = 51 - (1 \times 34)$ (from ④)

$= 51 - 1 \times (1768 - 34 \times 51)$ (by 3)

$= (1 \times 51) - (1 \times 1768) + 34 \times 51$

$= 35 \times 51 - 1 \times 1768$

$= 35 \times (1819 - 1 \times 1768) - 1 \times 1768$ (by 2)

$= 35 \times 1819 - 35 \times 1768 - 1 \times 1768$

$= 35 \times 1819 - 36 \times 1768$

$= 35 \times 1819 - 36 (3587 - 1 \times 1819)$

$= 35 \times 1819 - 36 \times 3587 + 36 \times 1819$

$= 71 \times 1819 - 36 \times 3587$

(2) gcd (12345, 54321) = 3

$3 = 3617 \times 12345 - 822 \times 54321$

② GCD (4076, 1024) = 4 $\Rightarrow$ $4 = 51 \times 4076 - 203 \times 1024$

④ Find integers m and n such that (i) $512m + 320n = 64$

Ans $512m + 320n = 64 \Rightarrow \gcd(512, 320) = 64$

Hence there will exist integers m and n so that the given equality holds good.

Use Euclidean algorithm to find m and n.

$512 = 1 \times 320 + 192$ (1)

$320 = 1 \times 192 + 128$ (2)

$192 = 1 \times 128 + 64$ (3)

$128 = 2 \times 64 + 0$

So $64 = 192 - 1 \times 128$ (from 3)

$= 192 - (320 - 1 \times 192)$ from 2

$= 192 - 320 + 1 \times 192$

$= 2 \times 192 - 320$

$= 2 \times (512 - 1 \times 320) - 320$

$= 2 \times 512 - 2 \times 320 - 320$

$= 2 \times 512 - 3 \times 320$

$64 = 512m + 320n \Rightarrow$ **m = 2 and n = -3**

(ii) $28844m + 15712n = 4$

$28844 = 1 \times 15712 + 13132$ (1)

$15712 = 1 \times 13132 + 2580$ (2)

$13132 = 5 \times 2580 + 232$ (3)

$2580 = 11 \times 232 + 28$ (4)

$232 = 8 \times 28 + 8$ (5)

$28 = 3 \times 8 + 4$

$8 = 2 \times 4 + 0$

$\Rightarrow 4 = 28 - 3 \times 8 = 28 - 3(232 - 8 \times 28)$ (From 5)

$= 25 \times 28 - 3 \times 232 = 25 \times (2580 - 11 \times 232) - 3 \times 232$ (4)

$= 25 \times 2580 - 278 \times 232 = 25 \times 2580 - 278 \times (13132 - 5 \times 2580)$ (3)

$= 1415 \times 2580 - 278 \times 13132 = 1415 (15712 - 13132) - 278 \times 13132$ (2)

$= 1415 \times 15712 - 1693 \times 13132 = 1415 \times 15712 - 1693 (28844 - 15712)$

$= 3108 \times 15712 - 1693 \times 28844 \Rightarrow$ **m = -1693, n = 3108**

Properties of GCD

① If $c \mid ab$ and a & c are coprime, then $c \mid b$.

Proof: Given a & c are coprime $\Rightarrow \gcd(a,c) = 1$

By previous theorem, there exists integers m and n such that ①

$$am + cn = \gcd(a,c) = 1$$

Multiplying by b throughout

$$amb + cnb = b.$$

Given $c \mid ab \Rightarrow c \mid m(ab)$ ⇒

Also $c \mid c(nb)$ → $2 \mid 6 \times 5$

$\Rightarrow c \mid mab + cnb$

$\Rightarrow c \mid b.$

$2 \mid (6 + 60)$ $2 \mid 66$

② If a and b are coprime and a and c are coprime, then a and bc are coprime.

proof: a and b are coprime $\Rightarrow \gcd(a,b) = 1$

$\Rightarrow am + bn = 1$

for some int m, n.

a and c are coprime $\Rightarrow \gcd(a,c) = 1$

$\Rightarrow pa + qc = 1.$

for some int p, q.

$(ma+nb) = 1$ and $(pa+qc) = 1$

Multiply ① & ②

$\Rightarrow (ma+nb)(pa+qc) = 1$

$\Rightarrow mpa^2 + mqac + npab + nqbc = 1.$

$\Rightarrow (\underbrace{map+nbp}_{\text{integer}} + qcm)a + (\underbrace{nq}_{\text{integer}})bc = 1$

This is of the form $ra + sbc = 1$ where r and s are integers.

$\Rightarrow \gcd(a, bc) = 1$

$\Rightarrow$ a and bc are coprime.

(8) If a, b are any integers, which are not simultaneously zero, and k is a positive integer then $\gcd(ka, kb) = k \cdot \gcd(a,b)$

Proof:- Let $\gcd(a,b) = d$

Then $ma + nb = d$ where m and n are integers.

$\Rightarrow (ma)k + (nb)k = dk$

$\Rightarrow m(ak) + n(bk) = kd$

$\Rightarrow \gcd(ak, bk) = k \cdot \gcd(a,b)$

If k is any integer, then the result becomes $\gcd(ka, kb) = |k| \gcd(a,b)$.

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

Proof: Since $\gcd(a,b)=d$ there exists integers m and n such that

$$am+bn=d$$

$$\Rightarrow \left(\frac{a}{d}\right)m+\left(\frac{b}{d}\right)n=1$$

Since $d|a$ and $d|b$, $\frac{a}{d}$ and $\frac{b}{d}$ are integers.

Hence $\left(\frac{a}{d}\right)m+\left(\frac{b}{d}\right)n=1 \Rightarrow \gcd\left(\frac{a}{d},\frac{b}{d}\right)=1$

(5) If $\gcd(a,b)=1$, then for any integer c,

$\gcd(ac,b)=\gcd(c,b)$

proof:- $\gcd(a,b)=1 \Rightarrow am_1+bn_1=1$ for integers m_1 and n_1.

Let $\gcd(ac,b)=d$. Then $(ac)m_2+bn_2=d$ for integers m_2 and n_2

(6) multiply

$$\Rightarrow (am_1+bn_1)(acm_2+bn_2)=d$$

$$\Rightarrow a^2m_1m_2c+abm_2n_1c+am_1n_2b+n_1n_2b^2=d$$

$$\Rightarrow a^2m_1m_2c+(acm_2n_1+am_1n_2+bn_1n_2)b=d$$

$$\Rightarrow m_3c+n_3b=d \Rightarrow \gcd(c,b)=d$$

$$\Rightarrow \gcd(ac,b)=\gcd(c,b)$$

6. If each of $a_1, a_2 \ldots a_n$ is coprime to b then the product $(a_1 a_2 \ldots a_n)$ is also coprime to b.

Proof: a_1 is coprime to $b \Rightarrow \gcd(a_1, b) = 1$

$\therefore$ By property 5

$$\gcd(a_1 a_2, b) = \gcd(a_2, b) = 1$$ (since a_2 & b are coprime.)

Again

$\gcd(a_1 a_2 a_3, b) = \gcd(a_3, b) = 1$ ($\because a_3, b$ are coprime)

Proceeding like this we have

$\gcd(a_1 a_2 a_3 \ldots a_n, b) = 1$

$\Rightarrow (a_1 a_2 \ldots a_n)$ and b are coprime.

Theorem:

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

Proof:- Let the prime factorisation of a and b be

$$a = p_1^{a_1} p_2^{a_2} \ldots p_n^{a_n}$$

$$b = p_1^{b_1} p_2^{b_2} \ldots p_n^{b_n}$$

Then $\gcd(a,b) = p_1^{\min(a_1,b_1)} \cdot p_2^{\min(a_2,b_2)} \cdots p_n^{\min(a_n,b_n)}$

and $\text{lcm}(a,b) = p_1^{\max(a_1,b_1)} \cdot p_2^{\max(a_2,b_2)} \cdots p_n^{\max(a_n,b_n)}$

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

Hence $\gcd(a,b) \times \text{lcm}(a,b)$

$= p_1^{[\min(a_1,b_1)+\max(a_1,b_1)]} p_2^{[\min(a_2,b_2)+\max(a_2,b_2)]} \cdots p_n^{[\min(a_n,b_n)+\max(a_n,b_n)]}$

$= p_1^{[a_1+b_1]} p_2^{[a_2+b_2]} \cdots p_n^{[a_n+b_n]}$

$= (p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n})(p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n})$

$= ab.$

23-9-22 A2

695 + 14 ½ marks.

(1) Using Euclidean algorithm, find gcd of (4076, 1024)

Sol

$4076 = 3 \times 1024 + 1004$

$1024 = 1 \times 1004 + 20$

$1004 = 50 \times 20 + 4$

$20 = 5 \times 4 + 0$

Since the last non-zero remainder is 4

i.e., $\gcd(4076, 1024) = 4$

Also

$4 = 1004 - 50 \times 20$

$= 1004 - 50[1024 - 1 \times 1004]$

$= 1004 - 50 \times 1024 + 50 \times 1004$

$= 51 \times 1004 - 50 \times 1024$

$= 51[4076 - 3 \times 1024] - 50 \times 1024$

$= 51 \times 4076 - 153 \times 1024 - 50 \times 1024$

$= 51 \times 4076 - 203 \times 1024$

$4 = 51 \times 4076 - 203 \times 1024.$