SRM INSTITUTE OF SCIENCE & TECHNOLOGY
(Deemed to be University u/s 3 of UGC Act, 1956)

SRM INSTITUTE OF SCIENCE AND TECHNOLOGY

RAMAPURAM PART- VADAPALANI CAMPUS, CHENNAI – 600 026

Department of Mathematics

Sub Title: DISCRETE MATHEMATICS FOR ENGINEERS

Sub Code: 18 MAB 302 T –Unit-2- Combinatorics and Number Theory

Combinatorics:

Combinatorics is the branch of mathematics which is related to counting. Combinatorics has many real life applications where counting of objects are involved. For example, we may be interested to know if there are enough mobile numbers to meet the demand or the number of allowable passwords in a computer system. It also deals with counting techniques and with optimization methods, that is, methods related to finding the best possible solution among several possibilities in a real problem. In this chapter we shall study counting problems in terms of ordered or unordered arrangements of objects. These arrangements are referred to as permutations and combinations. Combinatorics are largely used in the counting problems of Network communications, Cryptography, Network Security and Probability theory. We shall explore their properties and apply them to counting problems.

Fundamental principles of counting:

The Addition Rule :

Let us consider two tasks which need to be completed. If the first task can be Completed in M different ways and the second in N different ways, and if these cannot be performed simultaneously, then there are $M + N$ ways of doing either task. This is the addition rule of counting..

Example (1)

Suppose one girl or one boy has to be selected for a competition from a class comprising 17 boys and 29 girls. In how many different ways can this selection be made?

Solution:

The first task of selecting a girl can be done in 29 ways. The second task of selecting a boy can be done in 17 ways. It follows from the sum rule, that there are 17+29 = 46 ways of making this selection.

Example (2) :

A School library has 75 books on Mathematics, 35 books on Physics. A student can choose only one book. In how many ways a student can choose a book on Mathematics or Physics?

Solution:

(i) A student can choose a Mathematics book in “75” different ways.

(ii) A student can choose a Physics book in “35” different ways.

Hence applying the Rule of Sum, the number of ways a student can choose a book is 75 + 35 = 110.

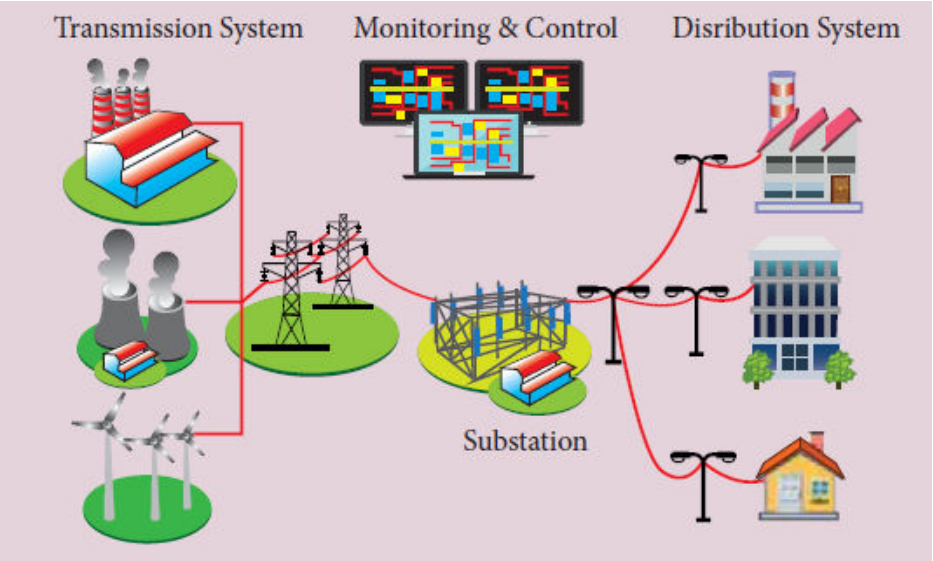
Example (3) :

If an electricity consumer has the consumer number say 238:110: 29, then describe

the linking and count the number of house connections upto the 29th consumer connection linked to the larger capacity transformer number 238 subject to the condition that each smaller capacity transformer can have a maximal consumer link of say 100.

Solution:

The following figure illustrates the electricity distribution network.



There are 110 smaller capacity transformers attached to a larger capacity transformer. As each smaller capacity transformer can be linked with only 100 consumers, we have for the 109 transformers; there will be $109 \times 100 = 10900$ links.

For the 110^{th} transformer there are only 29 consumers linked. Hence, the total number of consumers linked to the 238^{th} larger capacity transformer is $10900 + 29 = 10929$.

Note:

The sum rule may be extended to more than two tasks. Thus if there are n non-simultaneous tasks $T_1, T_2, T_3, \ldots, T_n$ which can be performed in $m_1, m_2, \ldots, m_n$ ways respectively, then the number of ways of doing one of these tasks is $m_1 + m_2 + \ldots + m_n$.

The Product Rule:

Let us suppose that a task comprises of two procedures. If the first procedure can be completed in M different ways and the second procedure can be done in N different ways after the first procedure is done, then the total number of ways of completing the task is $M \times N$.

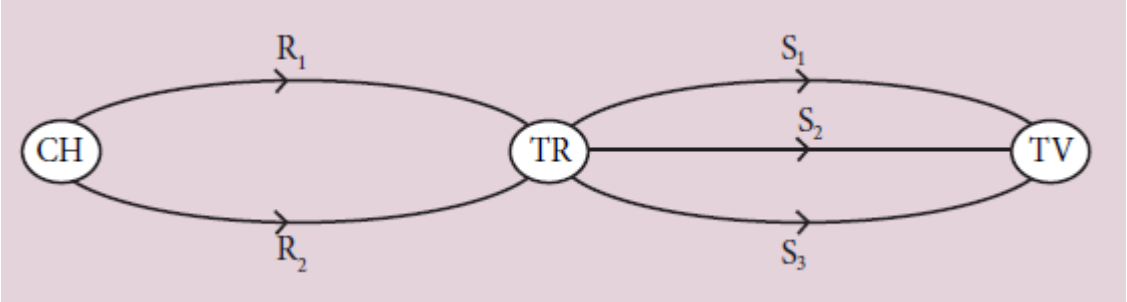
Example (1) :

Consider the 3 cities Chennai, Trichy and Tirunelveli. In order to reach Tirunelveli from Chennai, one has to pass through Trichy. There are 2 roads connecting Chennai with Trichy and there are 3 roads connecting Trichy with Tirunelveli. What is the total number of ways of travelling from Chennai to Tirunelveli?

Solution:

There are 2 roads connecting Chennai to Trichy. Suppose these are R_1 and R_2. Further there are 3 roads connecting Trichy to Tirunelveli . Let us name them as S_1, S_2 and S_3. Suppose a person chooses R_1 to travel from Chennai to Trichy and may further choose any of the 3 roads S_1, S_2 or S_3 to travel from Trichy to Tirunelveli. Thus the possible road choices are (R_1, S_1), (R_1, S_2), (R_1, S_3).

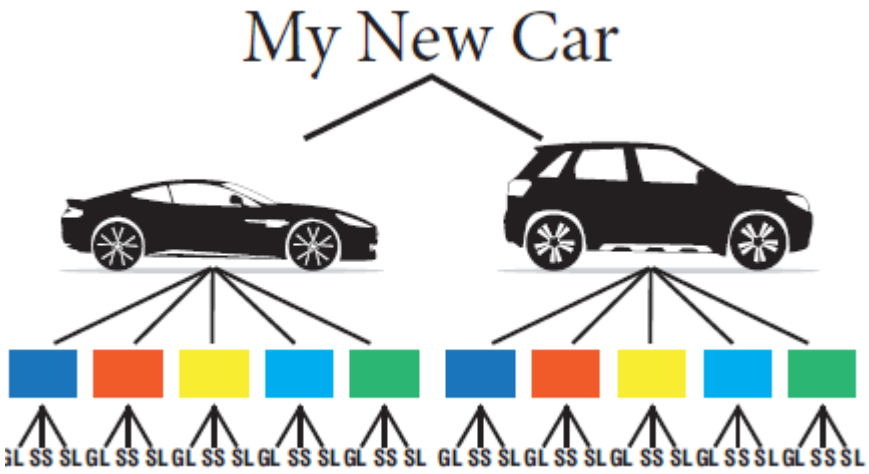
Similarly, if the person chooses R_2 to travel from Chennai to Trichy, the choices would be (R_2, S_1), (R_2, S_2), (R_2, S_3).



Thus there are $2 \times 3 = 6$ ways of travelling from Chennai to Tirunelveli.

Example (2) :

A person wants to buy a car. There are two brands of car available in the market and each brand has 3 variant models and each model comes in five different colours as in Figure In how many ways she can choose a car to buy?



Solution:

A car can be bought by choosing a brand, then a variant model, and then a colour. A brand can be chosen in 2 ways; a model can be chosen in 3 ways and a colour can be chosen in 5 ways.

By the rule of product the person can buy a car in $2 \times 3 \times 5 = 30$ different ways.

Example (3) :

A Woman wants to select one silk saree and one sungudi saree from a textile shop located at Kancheepuram. In that shop, there are 20 different varieties of silk sarees and 8 different varieties of sungudi sarees. In how many ways she can select her sarees?

Solution:

The work is done when she selects one silk saree and one sungudi saree. The Woman can select a silk saree in 20 ways and sungudi saree in 8 ways. By the rule of product, the total number of ways of selecting these 2 sarees is $20 \times 8 = 160$.

Note :

An extension of the product rule may be stated as follows:

If a task comprises of n procedures $P_1, P_2, P_3, \cdots, P_n$ which can be performed in $m_1, m_2, \cdots, m_n$ ways respectively, and procedure P_i can be done after procedures $P_1, P_2, P_3, \cdots, P_{i-1}$ are done, then the number of ways of completing the task is

$m_1 \times m_2 \times \cdots \times m_n$.

Permutations:

The number of distinct permutations of r objects which can be made from n distinct Objects is $\frac{n!}{(n-r)!}$ and it is denoted by nPr.

ie) $nPr = \frac{n!}{(n-r)!}$

Permutations of distinct objects:

In terms of function on any finite set say $S = \{x_1, x_2, \ldots x_n\}$, a permutation can be defined as a bijective mapping on the set S onto itself. The number of permutation on the set S is the same as the total number of bijective mappings on the set S.

No two things are together (Gap method):

To obtain the number of permutations of n different objects when no two of k given objects occur together and there are no restrictions on the remaining $m = n - k$ objects, we follow the procedure as follows:

- First of all, arrange the m objects on which there is no restriction in a row. These m objects can be permuted in ${}_mP_m = m!$ ways.
- Then count the number of gaps between every two of m objects on which there is no restriction including the end positions. Number of such gaps will be one more than m that is $(m+1)$. In this $m + 1$ gaps, we can permute the k objects in ${}_{m+1}P_k$ ways.
- Then the required number of ways is $m! \times {}_{(m+1)}P_k$.

Example (1) :

In how many ways 5 boys and 4 girls can be seated in a row so that no two girls are together.

Solution:

The 5 boys can be seated in the row in ${}_5P_5 = 5!$ ways.
In each of these arrangements 6 gaps are created.
Since no two girls are to sit together,
we may arrange 4 girls in this 6 gaps.
This can be done in ${}_6P_4$ ways.
Hence, the total number of seating arrangements is
$5! \times {}_6P_4 = 120 \times 360 = 43200$.

Example (2) :

There are 15 candidates for an examination. 7 candidates are appearing for mathematics examination while the remaining 8 are appearing for different subjects. In how many ways can they be seated in a row so that no two mathematics candidates are together?

Solution:

Let us arrange the 8-non-mathematics candidates in ${}_8P_8 = 8!$ Ways. Each of these arrangements create 9 gaps. Therefore, the 7 mathematics candidates can be placed in these 9 gaps in ${}_9P_7$ ways.
By the rule of product, the required number of arrangements is

$$8! \times {}_9P_7 = 8! \times \frac{9!}{(9-7)!}$$

The Inclusion-Exclusion Principle:

Suppose two tasks A and B can be performed simultaneously.
Let $n(A)$ and $n(B)$ represent the number of ways of performing the tasks A and B independent of each other. Also let $n(A \cap B)$ be the number of ways of performing the two tasks simultaneously. We cannot use the sum rule to count the number of ways of performing one of the tasks as that would lead to over counting. To obtain the correct number of ways we add the number of ways of performing each of the two tasks and then subtract the number of ways of doing both tasks simultaneously. This method is referred to as the principle of inclusion - exclusion. Using the notation of set theory we write it as

$$n(A \cup B) = n(A) + n(B) - n(A \cap B).$$

Example (1) :

In a village, out of the total number of people, 80 percentage of the people own Coconut groves and 65 percent of the people own Paddy fields. What is the minimum percentage of people own both?

Solution:

Let $n(C)$ denote the percentage of people who own the Coconut groves and $n(P)$ denote the percentage of people who own Paddy fields.

We are given $n(C) = 80$ and $n(P) = 65$.

By the rule of inclusion - exclusion ,

$n(C \cap P) = n(C) + n(P) - n(C \cup P)$.

The maximum value of $n(C \cup P)$ is 100.

Therefore, the minimum value of $n(C \cap P)$ is $80 + 65 - 100 = 45$.

That is, the minimum percentage of the people who own both is 45.

Example (2) :

A survey in 1986 asked households whether they had a VCR, a CD player or cable TV. 40 had a VCR. 60 had a CD player; and 50 had cable TV. 25 owned VCR and CD player. 30 owned a CD player and had cable TV. 35 owned a VCR and had cable TV. 10 households had all three. How many households had at least one of the three?

Solution:

let V be the set of households with a VCR. Let C be the set of households with a CD player. Let T be the set of households with cable TV. The question is asking for $V \cup C \cup T$.

By inclusion-exclusion, that is equal to

$$|V| + |C| + |T| - |V \cap C| - |V \cap T| - |C \cap T| + |V \cap C \cap T|$$

Therefore, $|V \cup C \cup T| = 40 + 60 + 50 - 25 - 30 - 35 + 10 = 70$

Example (3) :

A large software development company employs 100 computer programmers. Of them, 45 are proficient in Java, 30 in C#, 20 in Python, six in C# and Java, one in Java and Python, five in C# and Python, and just one programmer is proficient in all three languages above. Determine the number of computer programmers that are not proficient in any of these three languages.

Solution:

As done in the first inclusion-principle exercise problem above, start with defining the given information:

Let U denote the set of all employed computer programmers and let J, C and P denote the set of programmers proficient in Java, C# and Python, respectively. Thus:

$|U| = 100$, $|J| = 45$, $|C| = 30$, $|P| = 20$, $|J \cap C| = 6$, $|J \cap P| = 1$, $|C \cap P| = 5$

$|J \cap C \cap P| = 1$

Determine the number of computer programmers that are not proficient in any of these three languages.

In other words, we need to determine the cardinality of the complement of the set J ∪ C ∪ P. (This is denoted as |(J ∪ C ∪ P)'|). Calculate |J ∪ C ∪ P| first before determining the complement value:

$|J \cup C \cup P| = 39 + 5 + 20 + 4 + 15 + 1 = 84$

Now calculate the complement:

$|(J \cup C \cup P)'| = |U| - |J \cup C \cup P| = 100 - 84 = 16$

16 programmers are not proficient in any of the three languages

Example (4) : There are 350 farmers in a large region. 260 farm beetroot, 100 farm yams, 70 farm radish, 40 farm beetroot and radish, 40 farm yams and radish, and 30 farm beetroot and yams. Let B, Y, and R denote the set of farms that farm beetroot, yams and radish respectively. Determine the number of farmers that farm beetroot, yams, and radish.

Solution:

The letters for denoting the sets have already been provided in the question itself (unlike the above example). We may therefore note the cardinality straight away:

$|U| = 350$, $|B| = 260$, $|Y| = 100$, $|R| = 70$, $|B \cap R| = 40$, $|Y \cap R| = 40$, $|B \cap Y| = 30$

We need to determine the cardinality of the intersection of all three sets, which is $|B \cap Y \cap R|$. This is the unknown which we can assign determine algebraically.. Populate a Venn diagram with the given information. Use x to represent $|B \cap Y \cap R|$.

Let x farmers farm beetroot, yams, and radish. That is, let $|B \cap Y \cap R| = x$

Now solve for x algebraically:

$|U| = 350 = 190 + x + (30 - x) + x + (40 - x) + (40 - x) + 30 + x + x - 10$

$350 = 320 + x$

$x = 30$

Therefore, 30 farmers farm beetroot, yams, and radish.

Four events:

The generalization of these formulas to an arbitrary number of sets is called the inclusion-exclusion principle. Given sets A_1, A_2, … A_n, the cardinality of the union is: [The sum of the individual cardinalities, minus all the cardinalities of intersections of two sets, plus the cardinalities of intersections of three sets, minus the cardinalities of intersections of four sets, etc. This alternating sum ends with plus or minus the cardinality of the intersection of all n sets].

$$\mathbf{n}(A \cup B \cup C \cup D) = \mathbf{n}(A) + \mathbf{n}(B) + \mathbf{n}(C) + \mathbf{n}(D) - \mathbf{n}(A \cap B) - \mathbf{n}(A \cap C) - \mathbf{n}(A \cap D) - \mathbf{n}(B \cap C) - \mathbf{n}(B \cap D) - \mathbf{n}(C \cap D) + \mathbf{n}(A \cap B \cap C) + \mathbf{n}(A \cap B \cap D) + \mathbf{n}(A \cap C \cap D) + \mathbf{n}(B \cap C \cap D) - \mathbf{n}(A \cap B \cap C \cap D)$$.

Pigeon-hole 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.

Proof:

Let the n pigeons be labeled $P_1, P_2, \ldots, P_n$ and the m pigeonholes be labeled $H_1, H_2, \ldots, H_m$.

If $P_1, P_2, \ldots, P_m$ are assigned to $H_1, H_2, \ldots, H_m$ respectively,

we are left with the (n – m) pigeons $P_{m+1}, P_{m+2}, \ldots, P_n$.

If these left over pigeons are assigned to the m pigeonholes again in any random manner, at least one pigeonhole will contain two or more pigeons.

GENERALISATION OF THE PIGEONHOLE PRINCIPLE:

If n pigeons are accommodated in m pigeonholes 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.

Example (1):

A man hiked for 10 hours and covered a total distance of 45 km. It is known that he hiked 6 km in the first hour and only 3 km in the last hour. Show that he must have hiked at least 9 km within a certain period of 2 consecutive hours.

Solution:

Since, the man hiked 6 + 3 = 9 km in the first and last hours, he must have hiked 45 – 9 = 36 km during the period from second to ninth hours.

If we combine the second and third hours together, the fourth and fifth hours together, etc. and the eighth and ninth hours together, we have 4 time periods.

Let us now treat 4 time periods as pigeonholes and 36 km as 36 pigeons.

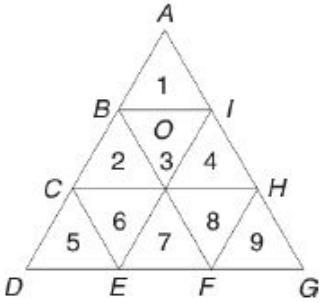
Using the generalized pigeonhole principal, the least no. of pigeons accommodated in one pigeonhole

$$= \left\lfloor \frac{36-1}{4} \right\rfloor + 1$$
$$= \lfloor 8.75 \rfloor + 1$$
$$= 8 + 1$$
$$= 9$$

Example (2)

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

Let ADG be the given equilateral triangle. The pairs of points B, C; E, F and H, I are the points of trisection of the sides AD, DG and GA respectively.



We have divided the triangle ADG into 9 equilateral triangles each of side $\frac{1}{3}$

The 9 sub-triangles may be regarded as 9 pigeonholes and 10 interior points may be regarded as 10 Pigeons.

Then by the pigeonhole principle, at least one sub triangle must contain 2 interior points.

The distance between any two interior points of any sub triangle cannot exceed the length of the side, namely, $\frac{1}{3}$

Hence the result.

Example (3) :

If n pigeonholes are occupied by (kn + 1) pigeons, where k is a positive integer, prove that at least one pigeonhole is occupied by (k + 1) or more pigeons.

Solution:

If at least one pigeonhole is not occupied by (k + 1) or more pigeons, each pigeonhole contains at most k pigeons.

Hence, the total number of pigeons occupying the n pigeonholes is at most kn.

But there are (kn + 1) pigeons.

This results in a contradiction. Hence, the result

Example (4):

Prove that in any group of six people, at least three must be mutual friends or at least three must be mutual strangers.

Solution:

Let A be one of the six people.

Let the remaining 5 people be accommodated in 2 rooms labeled "A's friends" and "strangers to A".

Treating 5 people as 5 pigeons and 2 rooms as pigeonholes, by the generalized pigeonhole principle, one of the rooms must contain

$$= \left\lfloor \frac{5-1}{2} \right\rfloor + 1 = 3 \text{ people.}$$

Let the room labeled "A's friends" contain 3 people. If any two of these 3 people are friends, then together with A, we have a set of 3 mutual friends.

If no two of these 3 people are friends, then these 3 people are mutual strangers.

In either case, we get the required conclusion.

If the room labeled "strangers to A" contains 3 people, we get the required

Conclusion by similar argument.

Example (5) :

In a group of 100 people, several will have birth days in the same month.At least how many must have birth days in the same month?

Solution:

Here number of pigeons (people) n = 100

Number of pigeons (months) m = 12

By geralized pigeon hole principle,

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

$$= \left\lfloor \frac{100-1}{12} \right\rfloor + 1 = \left\lfloor \frac{99}{12} \right\rfloor + 1$$

$$= \lfloor 8.25 \rfloor + 1 = 8 + 1 = 9$$

Example (6) :

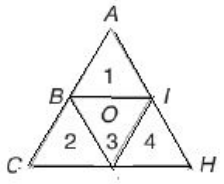
Of any 5 points chosen within an equilateral triangle whose sides are of length 1, show that two are

Within a distance of $\frac{1}{2}$ of each other.

Solution:

Let ACH be the given equilateral triangle. The pairs of points B, O and I are the points of

Intersection of the sides AC, CH and AH respectively.



We have divided the triangle ACH into 4 equilateral triangles each of side $\frac{1}{2}$

The 4 sub-triangles may be regarded as 4 pigeonholes and 5 interior points may be regarded as 5 Pigeons.

Then by the pigeonhole principle, at least one sub triangle must contain 2 interior points.

$$= \left\lfloor \frac{n-1}{m} \right\rfloor + 1 = \left\lfloor \frac{5-1}{4} \right\rfloor + 1 = 2$$

The distance between any two interior points of any sub triangle cannot exceed the length of the side, namely, $\frac{1}{2}$

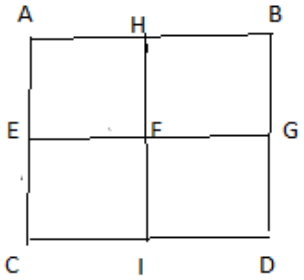
Hence the result.

Example (7) :

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.

Solution:

Let ABCD be the given square. The pairs of points E,F,g and H are the points of Intersection of the sides AB, BC,CD and DA respectively.



We have divided the square ABCD into 4 sub-squares each of side 1

The 4 sub-squares may be regarded as 4 pigeonholes and 5 interior points may be regarded as 5 Pigeons.

Then by the pigeonhole principle, at least one sub square must contain 2 interior points.

$$= \left\lfloor \frac{n-1}{m} \right\rfloor + 1 = \left\lfloor \frac{5-1}{4} \right\rfloor + 1 = 2$$

The distance between any two interior points of any sub square cannot exceed, namely $\sqrt{2}$,

Hence the result.

NUMBER THEORY

Divisibility:

Definition:

Assume 2 integers a and b, such that a ≠ 0 (a is not equal 0).

We say that 'a' divides'b' if there is an integer' c 'such that b = ac.

If a divides b we say that' a 'is a factor of' b' and that' b 'is multiple of'a'. •
The fact that a divides b is denoted as a | b.

Primes:

Definition:

A positive integer p that greater than 1 and that is divisible only by 1 and by itself (p) is called a prime.

Fundamental theorem of Arithmetic

Any positive integer greater than 1 can be expressed as a product of prime numbers.

Example: $765 = 3 \cdot 3 \cdot 5 \cdot 17 = 3^2 \cdot 5 \cdot 17.$

Primes and composites

- **How to determine whether the number is a prime or a composite?**

Let n be a number. Then in order to determine whether it is **a prime** we can test:

- **Approach 1:** if any number $x < n$ divides it. If yes it is a composite. If we test all numbers $x < n$ and do not find the proper divisor then n is a prime.
- **Approach 2:** if any prime number x < n divides it. If yes it is a composite. If we test all primes $x < n$ and do not find a proper divisor then n is a prime.
- **Approach 3:** if any prime number x $<\sqrt{n}$ divides it. If yes it is a composite. If we test all primes $x <\sqrt{n}$ and do not find a proper divisor then n is a prime.

The Sieve of Eratosthenes (276-194 BCE)

How to find all primes between 2 and n?

1. Write the numbers $2, \ldots, n$ into a list. Let $i := 2$.
2. Remove all strict multiples of i from the list.
3. Let k be the smallest number present in the list s.t. $k > i$. Then let $i := k$.
4. If $i > \sqrt{n}$ then stop else goto step 2.

Trial division: A very inefficient method of determining if a number n is prime, is to try every integer $i \leq \sqrt{n}$ and see if n is divisible by i.

Division

Let a be an integer and d a positive integer. Then there are unique integers, q and r, with 0 <= r < d, such that

a = dq + r.

Definitions:

- a is called the **dividend**,
- d is called the **divisor**,
- q is called the **quotient** and
- r the **remainder** of the division.

Example: a= 14, d = 3
14 = 3*4 + 2
14/3=3.666
14 div 3 = 4
14 mod 3 = 2

Relations:

- **q = a div d , r = a mod d**

Greatest common divisor

A systematic way to find the gcd using factorization:

- Let $a=p_1^{a1} p_2^{a2} p_3^{a3} \dots p_k^{ak}$ and $b= p_1^{b1} p_2^{b2} p_3^{b3} \dots p_k^{bk}$
- $\gcd(a,b)= p_1^{\min(a1,b1)} p_2^{\min(a2,b2)} p_3^{\min(a3,b3)} \dots p_k^{\min(ak,bk)}$

Examples:

- gcd(24,36) = ?
- $24 = 2*2*2*3=2^3*3$
- $36= 2*2*3*3=2^2*3^2$
- gcd(24,36) =

Least common multiple

Definition: Let a and b are two positive integers. The least common multiple of a and b is the smallest positive integer that is divisible by both a and b. The **least common multiple** is denoted as **lcm(a,b).**

Example:

- **What is lcm(12,9) =?**
- Give me a common multiple: …

Least common multiple

A systematic way to find the lcm using factorization:

- Let $a=p_1^{a1}\ p_2^{a2}\ p_3^{a3}\ \dots\ p_k^{ak}$ and $b=p_1^{b1}\ p_2^{b2}\ p_3^{b3}\ \dots\ p_k^{bk}$
- $lcm(a,b)=p_1^{\max(a1,b1)}\ p_2^{\max(a2,b2)}\ p_3^{\max(a3,b3)}\ \dots\ p_k^{\max(ak,bk)}$

Example:

- **What is lcm(12,9) =?**
- $12 = 2*2*3=2^2*3$
- $9=3*3=3^2$
- **lcm(12,9)** $= 2^2 * 3^2 = 4 * 9 =$ **36**

Gcd and Lcm by Prime Factorizations

Suppose that the prime factorizations of *a* and *b* are:

$$a = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}, \qquad b = p_1^{b_1} p_2^{b_2} \dots p_n^{b_n}$$

where each exponent is a nonnegative integer (possibly zero). Then

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

This number clearly divides *a* and *b*. No larger number can divide both *a* and *b*. Proof by contradiction and the prime factorization of a postulated larger divisor.

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

This number is clearly a multiple of *a* and *b*. No smaller number can be a multiple of both *a* and *b*. Proof by contradiction and the prime factorization of a postulated smaller multiple.

Factorization is a very inefficient method to compute *gcd* and *lcm*. The Euclidian algorithm is much better.

Euclid algorithm

Finding the greatest common divisor requires factorization

- $a=p_1^{a1} p_2^{a2} p_3^{a3} \dots p_k^{ak}$, $b=p_1^{b1} p_2^{b2} p_3^{b3} \dots p_k^{bk}$
- $gcd(a,b)= p_1^{\min(a1,b1)} p_2^{\min(a2,b2)} p_3^{\min(a3,b3)} \dots p_k^{\min(ak,bk)}$

- Factorization can be cumbersome and time consuming since we need to find all factors of the two integers that can be very large.

- Luckily a more efficient method for computing the gcd exists:
- It is called **Euclid's algorithm**
  - the method is known from ancient times and named after Greek mathematician Euclid.

Assume two numbers 287 and 91. We want gcd(287,91).

- First divide the larger number (287) by the smaller one (91)
- We get 287 = 3*91 +14

(1) Any divisor of 91 and 287 must also be a divisor of 14:

- 287 - 3*91 = 14
- Why? [ak – cbk] =r → (a-cb)k = r → (a-cb) = r/k (must be an integer and thus k divides r]

(2) Any divisor of 91 and 14 must also be a divisor of 287

- Why? 287 = 3 b k + dk → 287 = k(3b +d) → 287 /k = (3b +d) ← 287/k must be an integer
- **But then gcd(287,91) = gcd(91,14)**

Example 1:

- Find the greatest common divisor of 666 & 558

- gcd(666,558) = gcd(558,108) = gcd(108,18) = **18**

  666=1*558 + 108
  558=5*108 + 18
  108=6*18 + 0

Example 2:

- Find the greatest common divisor of 286 & 503:

- gcd(503,286) =gcd(286, 217) =gcd(217, 69) = gcd(69,10) =gcd(10,9) = gcd(9,1) =**1**

  503=1*286 + 217
  286=1*217 + 69
  217 = 3*69 + 10
  69 = 6*10 + 9
  10=1*9 + 1

Exercises

1. Use the prime factorizations of 860 and 1375 to compute $\gcd(860,1375)$.
2. Use the prime factorizations of 6300 and 1584 to compute $\gcd(6300,1584)$.
3. Use the prime factorizations of 1260 and 2640 to compute $\gcd(1260,2640)$.
4. Use the prime factorizations of 2373 and 1374 to compute $\gcd(2373,1374)$.
5. Use the division algorithm to compute $\gcd(6300,1584)$.
6. Use the division algorithm to compute $\gcd(1260,2640)$.
7. Use the division algorithm to compute $\gcd(2373,1374)$.
8. Use the prime factorizations of 75 and 124 to find $\text{lcm}(75,124)$.
9. Use the prime factorizations of 236 and 125 to find $\text{lcm}(236,125)$.
10. Use the prime factorizations of 84 and 118 to find $\text{lcm}(84,118)$.
11. Suppose $ab=900$ and $\text{lcm}(a,b)=300$. Give $\gcd(a,b)$.
12. Let $m,a,b\in\mathbb{N}$. Show that $\gcd(ma,mb)=m\gcd(a,b)$; i.e. the greatest common divisor satisfies a distributive property.
13. Let $a,b,c\in\mathbb{N}$. Show that $\gcd(\gcd(a,b),c)=\gcd(a,\gcd(b,c))$; i.e. the greatest common divisor satisfies an associative property.
14. Let $a\in\mathbb{N}$. Show that $\gcd(a,a)=a$; i.e. the greatest common divisor is idempotent.
15. Let $a,b\in\mathbb{N}$. Show that $\gcd(a,b)=\gcd(b,a)$; i.e. the greatest common divisor satisfies a commutative property.
16. Let $a,b\in\mathbb{N}$. Show that $\text{lcm}(a,\gcd(a,b))=a$ and $\gcd(a,\text{lcm}(a,b))=a$.
17. Let $a\in\mathbb{N}$. Show that $\text{lcm}(a,a)=a$; i.e. the least common multiple is idempotent.
18. Let $a,b\in\mathbb{N}$. Show that $\text{lcm}(a,b)=\text{lcm}(b,a)$; i.e. the least common multiple satisfies a commutative property.

19. Let $a,b,c \in \mathbb{N}$. Show that $\text{lcm}\big(\text{lcm}(a,b),c\big) = \text{lcm}\big(a,\text{lcm}(b,c)\big)$; i.e. the least common multiple satisfies an associative property.
20. Let $m,a,b \in \mathbb{N}$. Show that $\text{lcm}\big(ma,mb\big) = m\text{lcm}\big(a,b\big)$; i.e. the least common multiple satisfies a distributive property.

Solutions:

1. $860 = 2^2 \cdot 5 \cdot 43$ and $1375 = 5^3 \cdot 11$. Therefore;

$$\begin{aligned}\gcd(860,1375) &= (2)^{\min(0,2)}(5)^{\min(1,3)}(11)^{\min(0,1)}(43)^{\min(0,1)} \\ &= (2)^0(5)(11)^0(43)^0 \\ &= 5\end{aligned}$$

2. $6300 = 2^2 \cdot 5^2 \cdot 7 \cdot 9$ and $1584 = 2^4 \cdot 9 \cdot 11$. Therefore;

$$\begin{aligned}\gcd\big(6300,1584\big) &= (2)^{\min(2,4)} \cdot (5)^{\min(0,2)} \cdot (7)^{\min(0,1)} \cdot (9) \cdot (11)^{\min(0,1)} \\ &= 2^2 \cdot 9 = 36\end{aligned}$$

3. $1260 = 2^2 \cdot 5 \cdot 7 \cdot 9$ and $2640 = 2^4 \cdot 3 \cdot 5 \cdot 11$. Therefore;

$$\begin{aligned}\gcd\big(1260,2640\big) &= (2)^{\min(2,4)}(3)^{\min(0,1)}(5)(7)^{\min(0,1)}(9)^{\min(0,1)}(11)^{\min(0,1)} \\ &= (2)^2(5) = 20\end{aligned}$$

4. $2373 = 3 \cdot 7 \cdot 113$ and $1374 = 2 \cdot 3 \cdot 229$. Therefore;

$$\gcd\big(2373,1374\big) = (2)^0(3)(7)^0(113)^0(229)^0 = 3.$$

5. $\gcd\big(6300,1584\big)$

$$\begin{aligned}r_1 &= 6300 - (3)(1584) = 1548 \\ r_2 &= 1584 - (1)(1548) = 36 \\ r_3 &= 1548 - (43)36 = 0\end{aligned}$$

Thus; $\gcd\big(6300,1584\big) = 36$.

6.

$$r_1 = 2640 - (2)(1260) = 120$$
$$r_2 = 1260 - (10)(120) = 60$$
$$r_3 = 120 - (2)60 = 0$$

Consequently, $\gcd(1260, 2640) = 60$.

7.

$$r_1 = 2373 - (1)(1374) = 999$$
$$r_2 = 1374 - (1)(999) = 375$$
$$r_3 = 999 - (2)375 = 249$$
$$r_4 = 375 - (1)(249) = 126$$
$$r_5 = 249 - (1)(126) = 123$$
$$r_6 = 126 - (1)(123) = 3$$
$$r_7 = 123 - (41)(3) = 0$$

Hence, $\gcd(2373, 1374) = 3$.

8. $75 = 3 \cdot 5^2$ and $124 = 2^2 \cdot 31$.
Thus,

$$\begin{aligned} \operatorname{lcm}(75,124) &= (2)^{\max(2,0)}(3)^{\max(1,0)}(5)^{\max(2,0)}(31)^{\max(1,0)} \\ &= (2)^2(3)^1(5)^2(31)^1 \\ &= 9300 \end{aligned}$$

9. $236 = 2^2 \cdot 59$ and $125 = 5^3$.
Hence,

$$\begin{aligned} \operatorname{lcm}(236,125) &= (2)^{\max(2,0)}(5)^{\max(3,0)}(59)^{\max(1,0)} \\ &= (2)^2(5)^3(59)^1 \\ &= 29500 \end{aligned}$$

10. $84 = 2^2 \cdot 3 \cdot 7$ and $118 = 2 \cdot 59$.
Therefore,

$$\begin{aligned} \operatorname{lcm}(84,118) &= (2)^{\max(2,1)}(3)^{\max(1,0)}(7)^{\max(1,0)}(59)^{\max(1,0)} \\ &= (2)^2(3)^1(7)^1(59)^1 \\ &= 4956 \end{aligned}$$

11. Suppose $ab = 900$ and $\text{lcm}(a,b) = 300$. We know that $\text{lcm}(a,b)\gcd(a,b) = ab$.

So, $\gcd(a,b) = \dfrac{ab}{\text{lcm}(a,b)} = \dfrac{900}{300} = 3$. The greatest common divisor is:

$\gcd(a,b) = 3$.

12. Let $m, a, b \in \mathbb{N}$.

Suppose $p_1, p_2, ..., p_n$ are prime numbers so that $a = (p_1)^{\alpha_1}(p_2)^{\alpha_2}...(p_n)^{\alpha_n}$ and $b = (p_1)^{\beta_1}(p_2)^{\beta_2}...(p_n)^{\beta_n}$, where the values $\alpha_1, \alpha_2, ..., \alpha_n, \beta_1, \beta_2, ..., \beta_n$ are either natural numbers or 0. Then

$\gcd(a,b) = (p_1)^{\min(\alpha_1,\beta_1)}(p_2)^{\min(\alpha_2,\beta_2)}...(p_n)^{\min(\alpha_n,\beta_n)}$

We have: $ma = (m)(p_1)^{\alpha_1}(p_2)^{\alpha_2}...(p_n)^{\alpha_n}$ and $mb = (m)(p_1)^{\beta_1}(p_2)^{\beta_2}...(p_n)^{\beta_n}$.

So, the greatest common divisor is:

$$\begin{aligned}\gcd(ma,mb) &= (m)^{\min(1,1)}(p_1)^{\min(\alpha_1,\beta_1)}(p_2)^{\min(\alpha_2,\beta_2)}...(p_n)^{\min(\alpha_n,\beta_n)} \\ &= m(p_1)^{\min(\alpha_1,\beta_1)}(p_2)^{\min(\alpha_2,\beta_2)}...(p_n)^{\min(\alpha_n,\beta_n)} \\ &= m\gcd(a,b)\end{aligned}$$

Hence, the greatest common divisor satisfies a distributive property.

13. Let $a, b, c \in \mathbb{N}$.

Suppose $p_1, p_2, ..., p_n$ are prime numbers so that $a = (p_1)^{\alpha_1}(p_2)^{\alpha_2}...(p_n)^{\alpha_n}$, $b = (p_1)^{\beta_1}(p_2)^{\beta_2}...(p_n)^{\beta_n}$ and $c = (p_1)^{\gamma_1}(p_2)^{\gamma_2}...(p_n)^{\gamma_n}$, where the values $\alpha_1, \alpha_2, ..., \alpha_n, \beta_1, \beta_2, ..., \beta_n, \gamma_1, \gamma_2, ..., \gamma_n$ are either natural numbers or 0. Then

$\gcd(a,b) = (p_1)^{\min(\alpha_1,\beta_1)}(p_2)^{\min(\alpha_2,\beta_2)}...(p_n)^{\min(\alpha_n,\beta_n)}$ and

$\gcd(b,c) = (p_1)^{\min(\beta_1,\gamma_1)}(p_2)^{\min(\beta_2,\gamma_2)}...(p_n)^{\min(\beta_n,\gamma_n)}$.

$\gcd(\gcd(a,b),c) = (p_1)^{\min(\min(\alpha_1,\beta_1),\gamma_1)}(p_2)^{\min(\min(\alpha_2,\beta_2),\gamma_2)}...(p_n)^{\min(\min(\alpha_n,\beta_n),\gamma_n)}$ and

$\gcd(a,\gcd(b,c)) = (p_1)^{\min(\alpha_1,\min(\beta_1,\gamma_1))}(p_2)^{\min(\alpha_2,\min(\beta_2,\gamma_2))}...(p_n)^{\min(\alpha_n,\min(\beta_n,\gamma_n))}$.

Here, it is important to observe that
$\min(\min(\alpha_n,\beta_n),\gamma_n) = \min(\alpha_n,\min(\beta_n,\gamma_n)) = \min(\alpha_n,\beta_n,\gamma_n)$.
The reason behind this is; while comparing 3 natural numbers, you can start comparing from whichever you want. If you want to find the smallest of 5, 9 and 6, then arrange them in order; $5 < 6 < 9$. The smallest is 5, this does not change. So, it is not important if you compare 5 & 9 first and then the result with 6; or if you compare 6 & 9 first and then the result with 5.

Therefore, $\gcd(\gcd(a,b),c) = \gcd(a,\gcd(b,c))$; i.e. the greatest common divisor satisfies an associative property.

14. Let $a \in \mathbb{N}$. Show that $\gcd(a,a) = a$; i.e. the greatest common divisor is idempotent.

Suppose $p_1, p_2, ..., p_n$ are prime numbers so that $a = (p_1)^{\alpha_1}(p_2)^{\alpha_2}...(p_n)^{\alpha_n}$ where the values $\alpha_1, \alpha_2, ..., \alpha_n$ are either natural numbers or 0. Then $\gcd(a,a) = (p_1)^{\min(\alpha_1,\alpha_1)}(p_2)^{\min(\alpha_2,\alpha_2)}...(p_n)^{\min(\alpha_n,\alpha_n)}$ where, of course, $\min(\alpha_n,\alpha_n) = \alpha_n$. Hence,

$$\begin{aligned}\gcd(a,a) &= (p_1)^{\min(\alpha_1,\alpha_1)}(p_2)^{\min(\alpha_2,\alpha_2)}...(p_n)^{\min(\alpha_n,\alpha_n)} \\ &= (p_1)^{\alpha_1}(p_2)^{\alpha_2}...(p_n)^{\alpha_n} = a\end{aligned}$$

It is easier to see this result if we restate the question as "what is the greatest number that divides both a and a?". The answer is, of course, a itself.

15. Let $a,b \in \mathbb{N}$. Show that $\gcd(a,b) = \gcd(b,a)$; i.e. the greatest common divisor satisfies a commutative property.

Suppose $p_1, p_2, ..., p_n$ are prime numbers so that $a = (p_1)^{\alpha_1}(p_2)^{\alpha_2}...(p_n)^{\alpha_n}$ and $b = (p_1)^{\beta_1}(p_2)^{\beta_2}...(p_n)^{\beta_n}$, where the values $\alpha_1, \alpha_2, ..., \alpha_n, \beta_1, \beta_2, ..., \beta_n$ are either natural numbers or 0. Then

$$\gcd(a,b) = (p_1)^{\min(\alpha_1,\beta_1)}(p_2)^{\min(\alpha_2,\beta_2)}...(p_n)^{\min(\alpha_n,\beta_n)}$$

and

$$\gcd(b,a) = (p_1)^{\min(\beta_1,\alpha_1)}(p_2)^{\min(\beta_2,\alpha_2)}...(p_n)^{\min(\beta_n,\alpha_n)}.$$

The conclusion follows from the observation that $\min(\alpha_n,\beta_n) = \min(\beta_n,\alpha_n)$. Hence, $\gcd(a,b) = \gcd(b,a)$.

16. Let $a,b \in \mathbb{N}$.

Suppose $p_1, p_2, ..., p_n$ are prime numbers so that $a = (p_1)^{\alpha_1}(p_2)^{\alpha_2}...(p_n)^{\alpha_n}$ and $b = (p_1)^{\beta_1}(p_2)^{\beta_2}...(p_n)^{\beta_n}$, where the values $\alpha_1, \alpha_2, ..., \alpha_n, \beta_1, \beta_2, ..., \beta_n$ are either natural numbers or 0. Then $\operatorname{lcm}(a,b) = (p_1)^{\max(\alpha_1,\beta_1)}(p_2)^{\max(\alpha_2,\beta_2)}...(p_n)^{\max(\alpha_n,\beta_n)}$ and $\gcd(a,b) = (p_1)^{\min(\alpha_1,\beta_1)}(p_2)^{\min(\alpha_2,\beta_2)}...(p_n)^{\min(\alpha_n,\beta_n)}$.

$$\operatorname{lcm}(a,\gcd(a,b)) = (p_1)^{\max(\alpha_1,\min(\alpha_1,\beta_1))}(p_2)^{\max(\alpha_2,\min(\alpha_2,\beta_2))}...(p_n)^{\max(\alpha_n,\min(\alpha_n,\beta_n))}$$

Let's find $\max(\alpha_1, \min(\alpha_1, \beta_1))$. If $\alpha_1 < \beta_1$, then $\min(\alpha_1, \beta_1) = \alpha_1$ and $\max(\alpha_1, \min(\alpha_1, \beta_1)) = \max(\alpha_1, \alpha_1) = \alpha_1$. If $\beta_1 < \alpha_1$, then $\min(\alpha_1, \beta_1) = \beta_1$ and $\max(\alpha_1, \min(\alpha_1, \beta_1)) = \max(\alpha_1, \beta_1) = \alpha_1$. Similarly, for any n, $\max(\alpha_n, \min(\alpha_n, \beta_n)) = \alpha_n$. Therefore;

$$\begin{aligned}\operatorname{lcm}(a, \gcd(a,b)) &= (p_1)^{\max(\alpha_1, \min(\alpha_1, \beta_1))} (p_2)^{\max(\alpha_2, \min(\alpha_2, \beta_2))} \ldots (p_n)^{\max(\alpha_n, \min(\alpha_n, \beta_n))} \\ &= (p_1)^{\alpha_1} (p_2)^{\alpha_2} \ldots (p_n)^{\alpha_n} = a\end{aligned}$$

$$\gcd(a, \operatorname{lcm}(a,b)) = (p_1)^{\min(\alpha_1, \max(\alpha_1, \beta_1))} (p_2)^{\min(\alpha_2, \max(\alpha_2, \beta_2))} \ldots (p_n)^{\min(\alpha_n, \max(\alpha_n, \beta_n))}$$

With the reasoning we used above we can conclude that $\min(\alpha_n, \max(\alpha_n, \beta_n)) = \alpha_n$. Thus,

$$\begin{aligned}\gcd(a, \operatorname{lcm}(a,b)) &= (p_1)^{\min(\alpha_1, \max(\alpha_1, \beta_1))} (p_2)^{\min(\alpha_2, \max(\alpha_2, \beta_2))} \ldots (p_n)^{\min(\alpha_n, \max(\alpha_n, \beta_n))} \\ &= (p_1)^{\alpha_1} (p_2)^{\alpha_2} \ldots (p_n)^{\alpha_n} = a\end{aligned}$$

Hence, $\operatorname{lcm}(a, \gcd(a,b)) = a$ and $\gcd(a, \operatorname{lcm}(a,b)) = a$.

17. Let $a \in \mathbb{N}$. Suppose $p_1, p_2, \ldots, p_n$ are prime numbers so that $a = (p_1)^{\alpha_1} (p_2)^{\alpha_2} \ldots (p_n)^{\alpha_n}$ where the values $\alpha_1, \alpha_2, \ldots, \alpha_n$ are either natural numbers or 0. Then

$$\begin{aligned}\operatorname{lcm}(a,a) &= (p_1)^{\max(\alpha_1, \alpha_1)} (p_2)^{\max(\alpha_2, \alpha_2)} \ldots (p_n)^{\max(\alpha_n, \alpha_n)} \\ &= (p_1)^{\alpha_1} (p_2)^{\alpha_2} \ldots (p_n)^{\alpha_n} = a\end{aligned}$$

Therefore, $\operatorname{lcm}(a,a) = a$; i.e. the least common multiple is idempotent.

18. Let $a, b \in \mathbb{N}$. Suppose $p_1, p_2, \ldots, p_n$ are prime numbers so that $a = (p_1)^{\alpha_1} (p_2)^{\alpha_2} \ldots (p_n)^{\alpha_n}$ and $b = (p_1)^{\beta_1} (p_2)^{\beta_2} \ldots (p_n)^{\beta_n}$, where the values $\alpha_1, \alpha_2, \ldots, \alpha_n, \beta_1, \beta_2, \ldots, \beta_n$ are either natural numbers or 0. Then $\operatorname{lcm}(a,b) = (p_1)^{\max(\alpha_1, \beta_1)} (p_2)^{\max(\alpha_2, \beta_2)} \ldots (p_n)^{\max(\alpha_n, \beta_n)}$ and $\operatorname{lcm}(b,a) = (p_1)^{\max(\beta_1, \alpha_1)} (p_2)^{\max(\beta_2, \alpha_2)} \ldots (p_n)^{\max(\beta_n, \alpha_n)}$. Since $\max(\alpha_1, \beta_1) = \max(\beta_1, \alpha_1)$, we can conclude that $\operatorname{lcm}(a,b) = \operatorname{lcm}(b,a)$.

19. Let $a,b,c \in \mathbb{N}$. Suppose $p_1, p_2, ..., p_n$ are prime numbers so that $a = (p_1)^{\alpha_1}(p_2)^{\alpha_2}...(p_n)^{\alpha_n}$, $b = (p_1)^{\beta_1}(p_2)^{\beta_2}...(p_n)^{\beta_n}$ and $c = (p_1)^{\gamma_1}(p_2)^{\gamma_2}...(p_n)^{\gamma_n}$, where the values $\alpha_1, \alpha_2, ..., \alpha_n, \beta_1, \beta_2, ..., \beta_n, \gamma_1, \gamma_2, ..., \gamma_n$ are either natural numbers or 0. Then

$\text{lcm}(a,b) = (p_1)^{\max(\alpha_1,\beta_1)}(p_2)^{\max(\alpha_2,\beta_2)}...(p_n)^{\max(\alpha_n,\beta_n)}$ and

$\text{lcm}(b,c) = (p_1)^{\max(\beta_1,\gamma_1)}(p_2)^{\max(\beta_2,\gamma_2)}...(p_n)^{\max(\beta_n,\gamma_n)}$.

$\text{lcm}(\text{lcm}(a,b),c) = (p_1)^{\max(\max(\alpha_1,\beta_1),\gamma_1)}(p_2)^{\max(\max(\alpha_2,\beta_2),\gamma_2)}...(p_n)^{\max(\max(\alpha_n,\beta_n),\gamma_n)}$ and

$\text{lcm}(a,\text{lcm}(b,c)) = (p_1)^{\max(\alpha_1,\max(\beta_1,\gamma_1))}(p_2)^{\max(\alpha_2,\max(\beta_2,\gamma_2))}...(p_n)^{\max(\alpha_n,\max(\beta_n,\gamma_n))}$.

As we have pointed out before, the order at which you start to compare natural numbers does not matter;

$$\max(\max(\alpha_n,\beta_n),\gamma_n) = \max(\alpha_n,\max(\beta_n,\gamma_n)) = \max(\alpha_n,\beta_n,\gamma_n).$$

Hence, $\text{lcm}(\text{lcm}(a,b),c) = \text{lcm}(a,\text{lcm}(b,c))$; i.e. the least common multiple satisfies an associative property.

20. Let $m,a,b \in \mathbb{N}$.

Suppose $p_1, p_2, ..., p_n$ are prime numbers so that $a = (p_1)^{\alpha_1}(p_2)^{\alpha_2}...(p_n)^{\alpha_n}$ and $b = (p_1)^{\beta_1}(p_2)^{\beta_2}...(p_n)^{\beta_n}$, where the values $\alpha_1, \alpha_2, ..., \alpha_n, \beta_1, \beta_2, ..., \beta_n$ are either natural numbers or 0. Then

$\text{lcm}(a,b) = (p_1)^{\max(\alpha_1,\beta_1)}(p_2)^{\max(\alpha_2,\beta_2)}...(p_n)^{\max(\alpha_n,\beta_n)}$

We have: $ma = (m)(p_1)^{\alpha_1}(p_2)^{\alpha_2}...(p_n)^{\alpha_n}$ and $mb = (m)(p_1)^{\beta_1}(p_2)^{\beta_2}...(p_n)^{\beta_n}$.
So, the least common multiple is:

$$\begin{aligned}\text{lcm}(ma,mb) &= (m)^{\max(1,1)}(p_1)^{\max(\alpha_1,\beta_1)}(p_2)^{\max(\alpha_2,\beta_2)}...(p_n)^{\max(\alpha_n,\beta_n)} \\ &= m(p_1)^{\max(\alpha_1,\beta_1)}(p_2)^{\max(\alpha_2,\beta_2)}...(p_n)^{\max(\alpha_n,\beta_n)} \\ &= m\,\text{lcm}(a,b)\end{aligned}$$

Thus, $\text{lcm}(ma,mb) = m\text{lcm}(a,b)$; i.e. the least common multiple satisfies a distributive property.

Modular arithmetic

- In computer science we often care about the remainder of an integer when it is divided by some positive integer.

Problem: Assume that it is a midnight. What is the time on the 24 hour clock after 50 hours?

Answer: the result is 2am

How did we arrive to the result:

- Divide 50 with 24. The reminder is the time on the 24 hour clock.
  - $50 = 2*24 + 2$
  - so the result is 2am.

OBJECTIVES

1). In how many ways can 8 Indians,4 Americans and 4 English mens can be seated in a row so all person of the same nationality sit together?

a) 3! 4!8!4! b) 3! 8! c) 3! 4! D) 3! 3! 8! **Answer: a**

Solution:

Taking all person of same nationality as one person, then we will have only three people.
These three person can be arranged themselves in 3! Ways.
8 Indians can be arranged themselves in 8! Way.
4 American can be arranged themselves in 4! Ways.
4 Englishman can be arranged themselves in 4! Ways.
Hence, required number of ways = 3! 8! 4! 4! Ways.

2). How many permutations of the letters of the word APPLE are there?

a) 600 b) 120 c) 240 d) 60 **Answer: d**

Solution:

APPLE = 5 letters.
But two letters PP is of same kind.
Thus, required permutations,
=5!2!=1202=60

3). How many different words can be formed using all the letters of the word ALLAHABAD?

i). when vowels occupy the even positions ii) both L do not occur together.

a) 7560 , 60 , 4200 b) 7890 , 120 , 650 c) 7660 , 200 , 4444 d) 7670 , 240 , 444 **Answer: a**

Solution:

ALLAHABAD = 9 letters. Out of these 9 letters there is 4 A's and 2 L's are there.
So, permutations = $9!4!.2!$ $9!4!.2!$ = 7560

(a) There are 4 vowels and all are alike i.e. 4A's.
_2^{nd} _4^{th} _6^{th} _8^{th} _
These even places can be occupied by 4 vowels. In
$4!4!$ $4!4!$

= 1 Way.
In other five places 5 other letter can be occupied of which two are alike i.e. 2L's.
Number of ways = $5!2!$ $5!2!$ Ways.
Hence, total number of ways in which vowels occupy the even places = $5!2!$ $5!2!$ × 1 = 60 ways.

(b) Taking both L's together and treating them as one letter we have 8 letters out of which A repeats 4 times and others are distinct. These 8 letters can be arranged in $8!4!$ $8!4!$ = 1680 ways.
Also two L can be arranged themselves in 2! ways.
So, Total no. of ways in which L are together = 1680 × 2 = 3360 ways.
Now, Total arrangement in which L never occur together,
= Total arrangement - Total no. of ways in which L occur together.
= 7560 – 3360 = 4200 ways

4). In how many ways can 10 examination papers be arranged so that the best and worst papers never come together?
a) 8 x 9! b) 8 x 8! c) 7 x 9! d) 9 x 8! **Answer: a**

Solution:
No. of ways in which 10 paper can arranged is 10! Ways.
When the best and the worst papers come together, regarding the two as one paper, we have only 9 papers.
These 9 papers can be arranged in 9! Ways.
And two papers can be arranged themselves in 2! Ways.
No. of arrangement when best and worst paper do not come together,
= 10! - 9! × 2! = 9!(10 - 2) = 8 × 9!

5). In how many ways 4 boys and 3 girls can be seated in a row so that they are alternate.
a) 144 b) 288 c) 12 d) 256 **Answer: a**

Solution:
Let the Arrangement be, **B G B G B G B**
4 boys can be seated in 4! Ways
Girl can be seated in 3! Ways
Required number of ways, = 4! × 3! = 144

6). In how many ways 2 students can be chosen from the class of 20 students?
a) 190 b) 180 c) 240 d) 390 **Answer: a**

Solution:
Number of ways = $20C_2$ =20!2!×18!=20×192=190

7) Three gentle men and three ladies are candidates for two vacancies .A voter has to vote for two Candidates .In how many ways one cast his vote?
a) 9 b) 30 c) 36 d) 16 **Answer: d**

Solution:
There are 6 candidates and a voter has to vote for any two of them.
So, the required number of ways is, = $6C_2$ =6 ! / 2!×4!= 15

8). A question paper has two A and B each containing 10 questions , if a student has to choose 8 from part A and 5 from part B .In how many ways can he chooses questions?
a) 11340 b) 12750 c) 40 d) 320 **Answer: a**

Solution:

There 10 questions in part A out of which 8 question can be chosen as = 10C8

Similarly, 5 questions can be chosen from 10 questions of Part B as = 10C5

Hence, total number of ways,

$=10C_8 \times 10C_5 = 11340$

9). The number of triangles which can be formed by joining the angular points of a polygon of 8 sides as vertices.

a) 56 b) 24 c) 16 d) 8 **Answer: a**

Solution:

A triangle needs 3 points.

And polygon of 8 sides has 8 angular points.

Hence, number of triangle formed,

$= 8 C_3 = 56$

10). A drawer contains 12 red and 12 blue socks, all unmatched. A person takes socks out at random in the dark. How many socks must he take out to be sure that he has at least two blue socks?

a) 18 b) 35 c) 28 d) 14 **Answer: d**

Explanation: Given 12 red and 12 blue socks so, in order to take out at least 2 blue socks, first we need to take out 12 shocks (which might end up red in worst case) and then take out 2 socks (which would be definitely blue). Thus we need to take out total 14 socks.

11). The least number of computers required to connect 10 computers to 5 routers to guarantee 5 computers can directly access 5 routers is _____

a) 74 b) 104 c) 30 d) 67 **Answer: c**

Explanation: Since each 5 computer need directly connected with each router. So 25 connections + now remaining 5 computer, each connected to 5 different routers, so 5 connections = 30 connections. Hence, c1->r1, r2, r3, r4, r5

c2->r1, r2, r3, r4, r5 . c3->r1, r2, r3, r4, r5 . c4->r1, r2, r3, r4, r5 . c5->r1, r2, r3, r4, r5

c6->r1 . c7->r2 . c8->r3 . c9->r4 . c10->r5

Now, any pick of 5 computers will have a direct connection to all the 5 routers.

12). In a group of 267 people how many friends are there who have an identical number of friends in that group?

a) 266 b) 2 c) 138 d) 202 **Answer: b**

Explanation: Suppose each of the 267 members of the group has at least 1 friend. In this case, each of the 267 members of the group will have 1 to 267-1=266 friends. Now, consider the numbers from 1 to n-1 as holes and the n members as pigeons. Since there is n-1 holes and n pigeons there must exist a hole which must contain more than one pigeon. That means there must exist a number from 1 to n-1 which would contain more than 1 member. So, in a group of n members there must exist at least two persons having equal number of friends. A similar case occurs when there exist a person having no friends.

13). When four coins are tossed simultaneously, in _____ number of the outcomes at most two of the coins will turn up as heads.

a) 17 b) 28 c) 11 d) 43 **Answer: c**

Explanation: The question requires you to find number of the outcomes in which at most 2 coins turn up as heads i.e., 0 coins turn heads or 1 coin turns head or 2 coins turn heads. The number of outcomes in which 0 coins turn heads is ${}^4C_0 = 1$ outcome. The number of outcomes in which 1 coin turns head is ${}^4C_1 = 6$ outcomes. The number of outcomes in which 2 coins turn heads is,

${}^4C_2 = 15$ outcomes. Therefore, total number of outcomes = 1 + 4 + 6 = 11 outcomes.

14). How many numbers must be selected from the set {1, 2, 3, 4} to guarantee that at least one pair of these numbers add up to 7?

a) 14 b) 5 c) 9 d) 24 **Answer: b**

Explanation: With 2 elements pairs which give sum as 7 = {(1,6), (2,5), (3,4), (4,3)}. So choosing 1 element from each group = 4 elements (in worst case 4 elements will be either {1,2,3,4} or {6,5,4,3}). Now using pigeonhole principle = we need to choose 1 more element so that sum will definitely be 7. So Number of elements must be 4 + 1 = 5.

15). During a month with 30 days, a cricket team plays at least one game a day, but no more than 45 games. There must be a period of some number of consecutive days during which the team must play exactly _____ number of games.

a) 17 b) 46 c) 124 d) 24 **Answer: d**

Explanation: Let a1 be the number of games played until day 1, and so on, ai be the no games played until i. Consider a sequence like a1,a2,…a30 where $1 \le ai \le 45$, $\forall ai$. Add 14 to each element of the sequence we get a new sequence a1+14, a2+14, … a30+14 where, $15 \le ai+14 \le 59$, $\forall ai$. Now we have two sequences 1. a1, a2, …, a30 and 2. a1+14, a2+14, …, a30+14. having 60 elements in total with each elements taking a value ≤ 59. So according to pigeon hole principle, there must be at least two elements taking the same value ≤59 i.e., ai = aj + 14 for some i and j. Therefore, there exists at least a period such as aj to ai, in which 14 matches are played.

16). There are 10 points in a plane and 4 of them are collinear. The number of straight lines joining any two points is

(a) 45 (b) 40 (c) 39 (d) 38. **Ans :** b

17). Number of sides of a polygon having 44 diagonals is (a) 4 (b) 4! (c) 11 (d) 22 **Ans :** c

18). In a plane there are 10 points are there out of which 4 points are collinear, then the number of triangles formed is

(a) 110 (b) ${}_{10}C_3$ (c) 120 (d) 116 **Ans d**

18). In an examination there are three multiple choice questions and each question has 5 choices . Number of ways in which a student can fail to get all answer correct is

(a) 125 (b) 124 (c) 64 (d) 63 **Ans : b**

19) Assuming that repetitions are not permitted, how many four-digit numbers are less than 4000 , can be formed form the six digits 1, 2, 3, 5, 7, 8?

(a) 125 (b) 124 (c) 180 (d) 63 **Ans : c**

Explanation:

If a 4-digit number 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 one 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 x P(5, 3)

= 3 x 5 x 4 x 3 = 180.

20). How many bit strings of length 10 contain (a) exactly four 1's,

(a) 200 (b) 210 (c) 220 (d) 230 **Ans : b**

Explanation:

A bit string of length 10 can be considered to have 10 positions. These 10 positions should be filled with four 1's and six 0's No. of required bit strings = $\frac{10!}{4!\,6!} = 210$

21) If we select 10 points in the interior of an equilateral triangle of side 1, then there must be at least two

points whose distance apart is

a) $= \frac{1}{3}$ b) $< \frac{1}{3}$ c) $> \frac{1}{3}$ d) $\geq \frac{1}{3}$ **Ans : b**

22) In any group of six people, how many of at least ------- must be mutual friends or at least -------- must be Mutual strangers.

(a) 2 (b) 4 (c) 3 (d) 5 **Ans : c**

23) The Pascal's identity in the theory of combination is

a) $nC_{r-1} + nC_r = (n+1)C_r$ b) $nC_{r+1} + nC_r = (n+1)C_r$

b) c) $nC_{r-1} + nC_{r+1} = (n+1)C_r$ d) $nC_{r-1} + nC_r = (n+1)C_{r+1}$ **Ans : a**

24) The number of arrangements of all the six letters in the word **PEPPER** is

(a) 70 (b) 80 (c) 60 (d) 50 **Ans : c**

25) How many different outcomes are possible when 5 dice are rolled ?

(a) 452 (b) 152 (c) 352 (d) 252 **Ans : d**

26) In a group of 100 people, several will have birth days in the same month.At least how many must have birth days in the same month?

(a) 6 (b) 9 (c) 19 (d) 29 **Ans : b**

27) If 20 processors are interconnected and every processor is connected to at least one other, Then at least how many processors are directly connected to the same number of processors ?

(a) 2 (b) 3 (c) 4 (d) 1 **Ans : a**

28) Among 30 Computer Science students, 15 know JAVA, 12 know C++ and 5 know both. How many students know exactly one of the languages.

(a) 27 (b) 22 (c) 17 (d) 5 **Ans : c**

29). How many positive integers not exceeding 1000 are divisible by 7 or 11?

(a) 270 (b) 22 0 (c) 170 (d) 50 **Ans : b**

30) If there are 5 points inside a square of side length 2, prove that two of the points are within a distance of ---------- of each other.

a) $\sqrt{2}$ b) $\sqrt{3}$ c) $\sqrt{5}$ d) $\sqrt{7}$ **Ans : a**

31) Greatest Common Divisor of two numbers is 8 while their Least Common Multiple is 144. Then the other number if one number is 16.

(a) 108 (b) 96 (c) 72 (d) 36 **Ans : c**

32) LCM of two numbers is 138. But their GCD is 23. The numbers are in a ratio 1:6. Which is the largest number amongst the two?

(a) 46 (b) 138 (c) 69 (d) 23 **Ans : b**

33) The least common multiple of two numbers is 168 and highest common factor of them is 12. If the difference between the numbers is 60, what is the sum of the numbers?

(a) 108 (b) 96 (c) 122 (d) 144 **Ans : a**

34) If least common multiple of two numbers is 225 and the highest common factor is 5 then find the numbers when one of the numbers is 25?

(a) 75 (b) 65 (c) 15 (d) 45 **Ans : d**

35) The greatest number of four digits which is divisible by 15, 25, 40, 75 is

(a) 600 (b) 9000 (c) 9600 (d) 9400 **Ans : c**

36) When a number is divided by 893 the remainder is 193. What will be the remainder when it is divided by 47?

(a) 19 (b) 5 (c) 33 (d) 23 **Ans : b**

Explanation:

In such cases and sums, simply follow these easy steps

Number is divided by 893. **Remainder = 193.**

Also, we observe that 893 is exactly divisible by 47.

So now simply divide the remainder by 47.

47	193	**4**
	-188	
	05	

So remainder is 5

37) The greatest length of the scale that can measure exactly 30 cm, 90 cm, 1 m 20 cm and 1 m 35 cm lengths Is

(a) 5 cm (b) 10 cm (c) 15 cm (d) 30 cm **Ans : c**

38) A Least Common Multiple of a, b is defined as _____

(a) It is the smallest integer divisible by both a and b

(b) It is the greatest integer divisible by both a and b

(c) It is the sum of the number a and b

(d) It is the difference of the number a and b **Ans : a**

39) If a, b are integers such that a > b then lcm(a, b) lies in _____

(a) a> lcm(a, b) > b (b) a > b >lcm(a, b) (c) lcm(a, b) ≥ a> b (d) b > lcm(a, b) < b **Ans : c**

40) The product of two numbers are 12 and their Greatest common divisor is 2 then LCM is?

(a) 12 (b) 2 (c) 6 (d) 16 **Ans : c**

41) If LCM of two number is 14 and GCD is 1 then the product of two numbers is?

(a) 14 (b) 15 (c) 7 (d) 49 **Ans : a**

42) If 'a' is $2^2 \times 3^1 \times 5^0$ and 'b' is $2^1 \times 3^1 \times 5^1$ then lcm of a , b is

(a) $2^2 \times 3^1 \times 5^1$ (b) $2^2 \times 3^2 \times 5^2$ (c) $2^3 \times 3^1 \times 5^0$ (d) $2^2 \times 3^2 \times 5^0$ **Ans : a**

43) The lcm of two prime numbers a and b is

(a) a /b (b) ab (c) a+b (d) 1 **Ans : b**

44) The prime factorization of 7007 is _____

(a) $7^3 \times 11 \times 13$ (b) $7^2 \times 11 \times 13$ (c) $7 \times 11 \times 13$ (d) $7 \times 11^3 \times 13$ **Ans : b**

45) Which positive integer less than 21 are relatively prime to 21?

(a) 18 (b) 19 (c) 21 (d) 24 **Ans : b**

46) The greatest common divisor of 3^{13}, $5^{17}$and 2^{12},3^5 is _____

(a) 3^0 (b) 3^1 (c) 3^3 (d) 3^5 **Ans : d**

47) The greatest common divisor of 0 and 5 is _____

(a) 0 (b) 1 (c) 2 (d) 5 **Ans : b**

Explanation: $\gcd(0, 5) = 0^{\min(1, 0)}.5^{\min(0, 1)}$.

48) The lcm of 3 and 21 is _____ if gcd(3,21)=3.

(a) 3 (b) 12 (c) 21 (d) 42 **Ans : c**

49) 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 **Ans : a**

50) 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 **Ans : a**