

Given an integral number **N**. The task is to find the count of digits present in this number.

Let's say:

**N = 2019**

Number of digits in N here is 4 and,  
the digits are: 2, 0, 1, 9.

**Some more Examples:**

**N = 1567**

Number of digits = 4

**N = 256**

Number of digits = 3

**N = 58964**

Number of digits = 5

## Solution 1

**Simple Solution:** A Simple Solution that comes in mind is:

1. Check if the number N is not equals to zero.
2. Increase the count of digits by 1 if N is not zero.
3. Reduce the number by dividing it by 10.
4. Repeat the above steps until the number is reduced to zero.

**Dry-run of above algorithm:** Consider an example, N = 58964. Initialize a variable **digitsCount** to zero which will store the count of digits. Keep incrementing *digitsCount* until N is not zero, and reduce it by dividing by 10 at each step.

**Iteration 1:** N **not equals** to 0

Increment digitsCount, digitsCount = digitsCount + 1.

digitsCount = 0 + 1 = 1.

N = N/10 = 58964/10 = 5896.

**Iteration 2:** N **not equals** to 0

Increment digitsCount, digitsCount = digitsCount + 1.

digitsCount = 1 + 1 = 2.

N = N/10 = 5896/10 = 589.

**Iteration 3:** N **not equals** to 0  
Increment digitsCount, digitsCount = digitsCount + 1.  
digitsCount = 2 + 1 = 3.  
N = N/10 = 589/10 = 58.

**Iteration 4:** N **not equals** to 0  
Increment digitsCount, digitsCount = digitsCount + 1.  
digitsCount = 3 + 1 = 4.  
N = N/10 = 58/10 = 5.

**Iteration 5:** N **not equals** to 0  
Increment digitsCount, digitsCount = digitsCount + 1.  
digitsCount = 4 + 1 = 5.  
N = N/10 = 5/10 = 0.

**Iteration 6:** N becomes equal to 0.  
Terminate any further operation.  
Return value of digitsCount.

Therefore, number of digits = 5.

**Analysis of above algorithm:** You can clearly see that, the number of operations performed in the above solution is equal to the count of digits present in the number. So, the time complexity of the solution is **O(digitsCount)**.

## Solution 2

**Better Solution:** A better solution is to use mathematics to solve this problem. The number of digits in a number say N can be easily obtained by using the formula:

number of digits in N =  $\log_{10}(N) + 1$ .

**Derivation:** Suppose the number of digits in the number N is K.

Therefore, we can say that:

$$10^{K-1} \leq N < 10^K$$

Applying base-10 logarithm to both sides in the above equation, we get:

$$K-1 \leq \log_{10}(N) < K.$$

$$\text{or, } K - 1 + 1 \leq \log_{10}(N) + 1 < K + 1$$

$$\text{or, } K \leq \log_{10}(N) + 1 < K + 1$$

Therefore,

$$K = \text{floor}(\log_{10}(N) + 1)$$

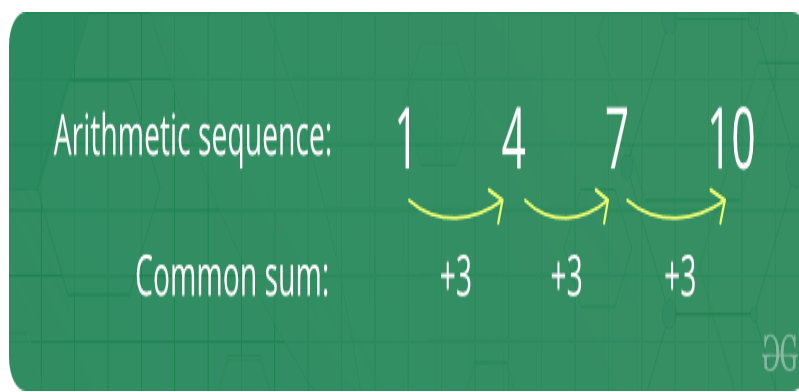
**Analysis of above algorithm:** Since the above algorithm works in a single operation by

using two mathematical operations, finding logarithmic and floor value. Therefore, the time complexity of the solution is  **$O(1)$** .

### Arithmetic and Geometric Progressions

## Arithmetic Progression

A sequence of numbers is said to be in an **Arithmetic progression** if the difference between any two consecutive terms is always the **same**. In simple terms, it means that the next number in the series is calculated by adding a fixed number to the previous number in the series. For example, 2, 4, 6, 8, 10 is an AP because difference between any two consecutive terms in the series (common difference) is same ( $4 - 2 = 6 - 4 = 8 - 6 = 10 - 8 = 2$ ).

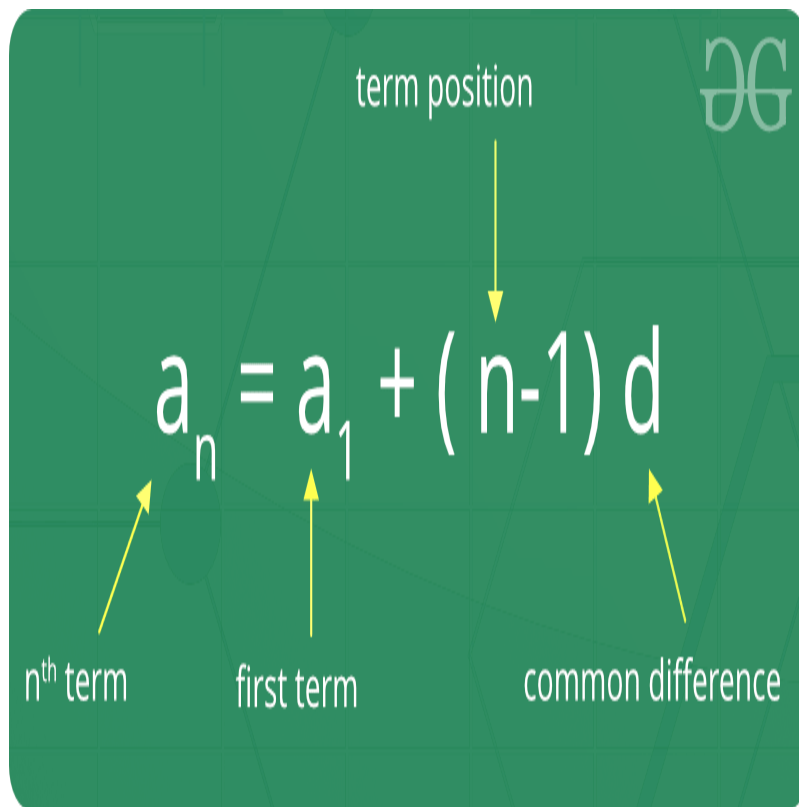


### Facts about Arithmetic Progression :

1. **Initial term:** In an arithmetic progression, the first number in the series is called the initial term.
2. **Common difference:** The value by which consecutive terms increase or decrease is called the common difference.
3. The behavior of the arithmetic progression depends on the common difference  $d$ . If the common difference is positive, then the members (terms) will grow towards positive infinity or negative, then the members (terms) will grow towards negative infinity.

### Formula of $n^{\text{th}}$ term of an A.P :

If 'a' is the initial term and 'd' is the common difference. Thus, the explicit formula is:



term position

$$a_n = a_1 + (n-1)d$$

$a_n$  is labeled as the  $n^{\text{th}}$  term.  
 $a_1$  is labeled as the first term.  
 $(n-1)$  is labeled as the term position.  
 $d$  is labeled as the common difference.

**Formula of sum of first n term of A.P:**

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

$S_n$  → Sum of a term of A.P.

$a$  → First term of A.P.

$d$  → Common difference

$n$  → Number of terms

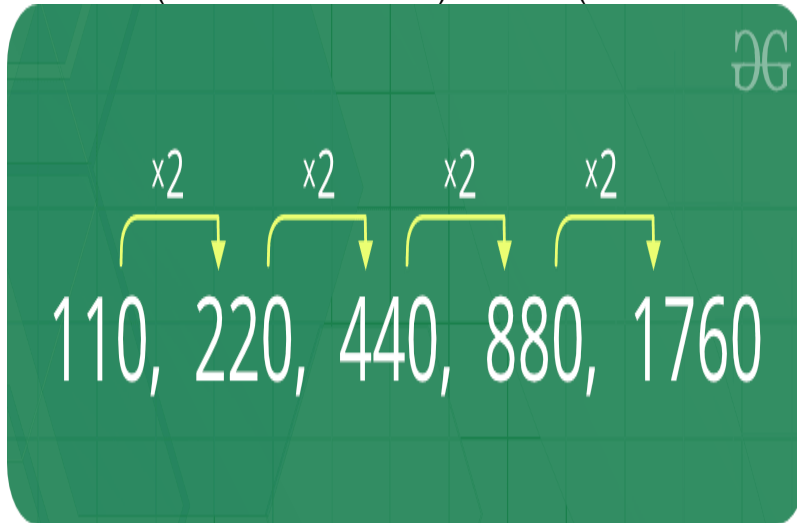


**General Formulas to solve problems related to Arithmetic Progressions:** If 'a' is the first term and 'd' is the common difference:

- **nth term** of an AP =  $a + (n-1)d$ .
- **Arithmetic Mean** = Sum of all terms in the AP / Number of terms in the AP.
- **Sum of 'n' terms** of an AP =  $0.5 n$  (first term + last term) =  $0.5 n [2a + (n-1)d]$ .

## Geometric Progression

A sequence of numbers is said to be in a **Geometric progression** if the ratio of any two consecutive terms is always same. In simple terms, it means that next number in the series is calculated by multiplying a fixed number to the previous number in the series. For example, 2, 4, 8, 16 is a GP because ratio of any two consecutive terms in the series (common difference) is same ( $4 / 2 = 8 / 4 = 16 / 8 = 2$ ).



#### Facts about Geometric Progression :

1. **Initial term:** In a geometric progression, the first number is called the initial term.
2. **Common ratio:** The ratio between a term in the sequence and the term before it is called the "common ratio."
3. The behaviour of a geometric sequence depends on the value of the common ratio. If the common ratio is:
  - Positive, the terms will all be the same sign as the initial term.
  - Negative, the terms will alternate between positive and negative.
  - Greater than 1, there will be exponential growth towards positive or negative infinity (depending on the sign of the initial term).
  - 1, the progression is a constant sequence.
  - Between -1 and 1 but not zero, there will be exponential decay towards zero.
  - -1, the progression is an alternating sequence.
  - Less than -1, for the absolute values there is exponential growth towards (unsigned) infinity, due to the alternating sign.

**Formula of  $n^{\text{th}}$  term of a Geometric Progression :** If 'a' is the first term and 'r' is the common ratio. Thus, the explicit formula is:

Same General Term

$$a_n = a_1 * r^{n-1}$$

General Term      First Term      Common Ratio

**Formula of sum of  $n^{\text{th}}$  term of Geometric Progression:**

$$\text{Sum} = \frac{a(r^n - 1)}{r - 1}$$

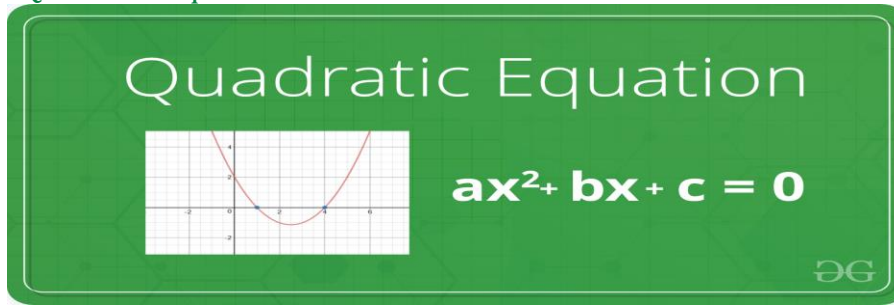
$r$  → Common ratio  
 $n$  → Number of terms  
 Sum → Sum of all Geometric Progression

**General Formulas to solve problems related to Geometric Progressions:**

If 'a' is the first term and 'r' is the common ratio:

- **$n^{\text{th}}$  term of a GP** =  $a * r^{n-1}$ .
- **Geometric Mean** =  $n^{\text{th}}$  root of product of  $n$  terms in the GP.
- **Sum of 'n' terms** of a GP ( $r < 1$ ) =  $[a (1 - r^n)] / [1 - r]$ .
- **Sum of 'n' terms** of a GP ( $r > 1$ ) =  $[a (r^n - 1)] / [r - 1]$ .
- **Sum of infinite terms** of a GP ( $r < 1$ ) =  $(a) / (1 - r)$ .

## Quadratic Equations



A **quadratic equation** is a second-order polynomial equation of a variable say **x**. The general form of a quadratic equation is given as:

$$a \cdot x^2 + b \cdot x + c = 0$$

Where  $a, b$  and  $c$  are real known values and,  $a$  can't be zero.

**Roots of an Equation:** The roots of an equation are the values for which the equation satisfies the given condition. For Example, the roots of equation  $x^2 - 7x - 12 = 0$  are 3 and 4 respectively. If we replace the value of  $x$  by 3 and 4 individually in the equation, the equation will evaluate to zero.

**A quadratic equation has two roots.** The roots of a quadratic equation can be easily obtained using the quadratic formula:

$$\text{roots} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

### Derivation:

$$ax^2 + bx + c = 0$$

$$\text{or, } ax^2 + bx = -c$$

$$\text{or, } x^2 + (b/a)x = -(c/a)$$

$$\text{or, } x^2 + (b/a)x + (b^2/4a^2) - (b^2/4a^2) = -(c/a)$$

$$\text{or, } x^2 + (b/a)x + (b^2/4a^2) = -(c/a) + (b^2/4a^2)$$

$$\text{or, } (x + b/2a)^2 = -(c/a) + (b^2/4a^2)$$

$$\text{or, } (x + b/2a)^2 = (b^2 - 4ac) / 4a^2$$

$$\text{or, } (x + b/2a) = \pm \sqrt{(b^2 - 4ac) / 4a^2}$$

$$\text{or, } x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

There arises **three cases** as described below while finding the roots of a quadratic



equation:

If  $b^2 < 4ac$ , then roots are complex (not real).

For example roots of  $x^2 + x + 1$ , roots are  $-0.5 + i1.73205$  and  $-0.5 - i1.73205$

If  $b^2 = 4ac$ , then roots are real and both roots are same.

For example, roots of  $x^2 - 2x + 1$  are 1 and 1

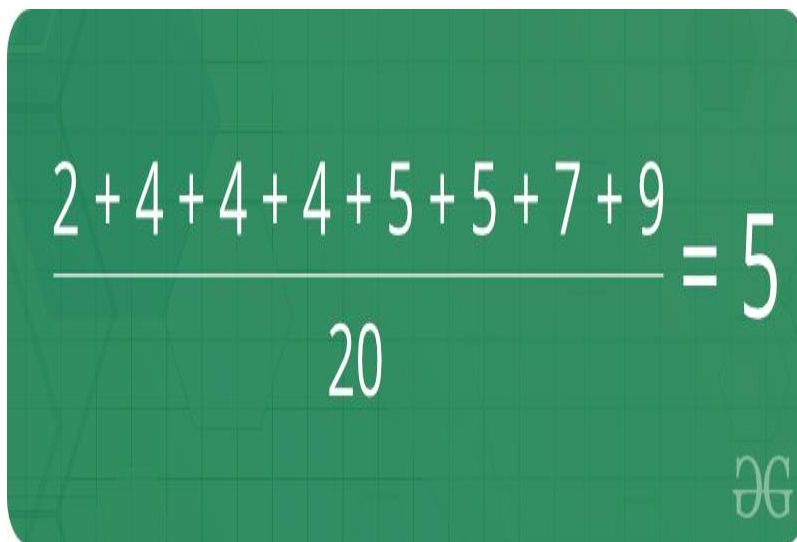
If  $b^2 > 4ac$ , then roots are real and different.

For example, roots of  $x^2 - 7x - 12$  are 3 and 4

### Mean and Median

## Mean

**Mean** is defined as average of a given set of data. Let us consider the sequence of numbers **2, 4, 4, 4, 5, 5, 7, 9**, the mean (average) of this given sequence is 5.


$$\frac{2+4+4+4+5+5+7+9}{8} = 5$$

$$\bar{X} = \frac{X_1 + X_2 + \dots + X_n}{n}$$

**Formula for finding Mean:**

Where,  $x_1, x_2, \dots, x_n$  denotes the terms of the given sequence and  $n$  is the count of numbers present in the given sequence.

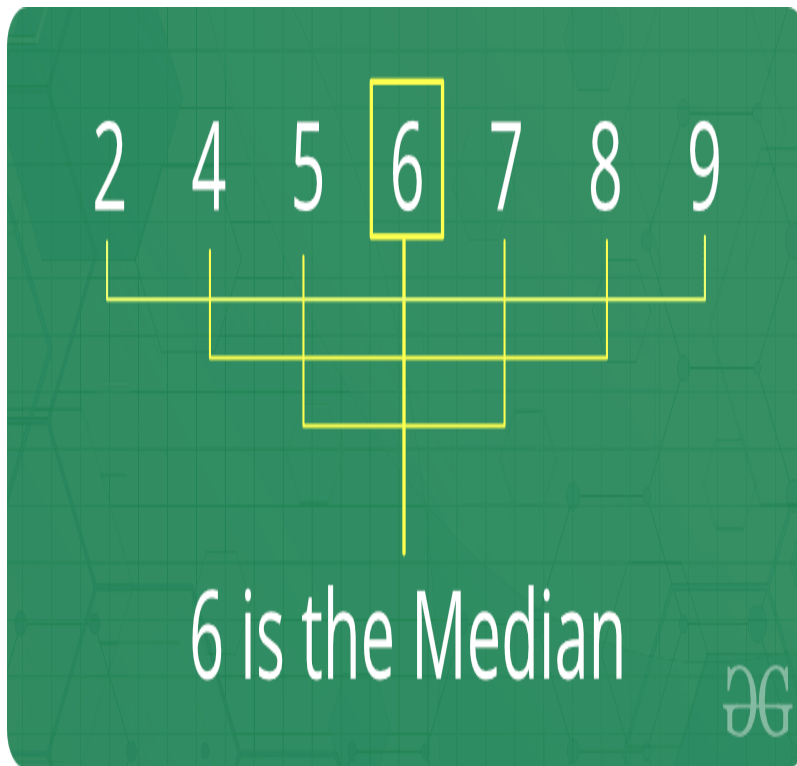
**Facts about Mean :**

1. The mean (or average) is the most popular and well known measure of central tendency.
2. It can be used with both discrete and continuous data, although its use is most often with continuous data.
3. There are other types of means. Geometric mean, Harmonic mean and Arithmetic mean.
4. Mean is the only measure of central tendency where the sum of the deviations of each value from the mean is always zero.

## Median

**Median** is the middle value of a set of data. To determine the median value in a sequence of numbers, the numbers must first be arranged in an ascending order.

- If the count of numbers in the sequence is ODD, the median value is the number that is in the middle, with the same amount of numbers below and above.
- If the count of numbers in the sequence is EVEN, the median is the average of the two middle values.



### Formula for finding Median :

- If the count of numbers is odd: After sorting the sequence,

Median =  $\{(N+1)/2\}^{\text{th}}$  value.

- If the count of numbers is even: After sorting the sequence,

Median = Average of  $(N/2)^{\text{th}}$  and  $\{(N/2) + 1\}^{\text{th}}$  value.

### Facts about Median :

1. Median is an important measure (compared to mean) for distorted data, because median is not so easily distorted. For example, median of {1, 2, 2, 5, 100} is 2 and mean is 22.
2. If the user adds a constant to every value, the mean and median increases by the same constant.
3. If the user multiplies every value by a constant, the mean and the median will also be multiplied by that constant.

### Prime Numbers

A **prime number** is a whole number greater than 1, which is only divisible by 1 and itself. First few prime numbers are : 2 3 5 7 11 13 17 19 23 .....



**Naive Method to Check if a number is Prime:** Since a number is prime only if it is divisible by 1 and the number itself, the naive method to check for primality of a number would be to iterate from 1 to N and check if there aren't any factors of N except and 1 and N itself.

**Algorithm:**

1. If, N is less than 2. It is not prime, return False.
2. Else:
  - Iterate from 2 to N-1 and check if any of the numbers between 2 and N-1 (both inclusive) divides N or not. If yes, then N is not prime, return False.
  - Otherwise, return True.

**Analysis of the above algorithm:** Since we are traversing linearly from 2 to N-1, the time complexity of the above algorithm will be linear **O(N)**.

## Sieve of Eratosthenes

Using **Sieve of Eratosthenes** is the most efficient way of generating prime numbers upto a given number N.

Following is the algorithm to find all the prime numbers less than or equal to a given integer  $n$  by Eratosthenes' method:

1. Create a list of consecutive integers from 2 to  $n$ : (2, 3, 4, ...,  $n$ ).
2. Initially, let  $p$  equal 2, the first prime number.
3. Starting from  $p^2$ , count up in increments of  $p$  and mark each of these numbers greater than or equal to  $p^2$  itself in the list. These numbers will be  $p(p+1)$ ,  $p(p+2)$ ,  $p(p+3)$ , etc..

- Find the first number greater than  $p$  in the list that is not marked. If there was no such number, stop. Otherwise, let  $p$  now equal this number (which is the next prime), and repeat from step 3.

**Explanation with Example:** Let us take an example when  $n = 50$ . So we need to print all print numbers smaller than or equal to 50.

We create a list of all numbers from 2 to 50.

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50

According to the algorithm we will mark all the numbers which are divisible by 2 and are greater than or equal to the square of it.

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50

Now we move to our next unmarked number 3 and mark all the numbers which are multiples of 3 and are greater than or equal to the square of it.

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50

We move to our next unmarked number 5 and mark all multiples of 5 and are greater than or equal to the square of it.

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50

We continue this process and our final table will look like below:

	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50

So the prime numbers are the unmarked ones: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47.

### LCM and HCF

**Factors and Multiples** : All numbers that divide a number completely, i.e., without leaving any remainder, are called factors of that number. For example, 24 is completely divisible by 1, 2, 3, 4, 6, 8, 12, 24. Each of these numbers is called a factor of 24 and 24 is called a multiple of each of these numbers.

**LCM** : LCM stands for *Least Common Multiple*. The lowest number which is exactly divisible by each of the given numbers is called the least common multiple of those numbers. For example, consider the numbers 3, 31 and 62 ( $2 \times 31$ ). The LCM of these numbers would be  $2 \times 3 \times 31 = 186$ .

To find the **LCM of the given numbers**, express each number as their prime factorization. The product of highest power of the prime numbers that appear in the prime factorization of any of the numbers gives us the LCM.

For example, consider the numbers 2, 3, 4 ( $2 \times 2$ ), 5, 6 ( $2 \times 3$ ). The LCM of these numbers is  $2 \times 2 \times 3 \times 5 = 60$ . The highest power of 2 comes from prime factorization of 4, the highest power of 3 comes from prime factorization of 3 and prime factorization of 6 and the highest power of 5 comes from prime factorization of 5.

**HCF** : The term HCF stands for *Highest Common Factor*. The largest number that divides two or more numbers is the highest common factor (HCF) for those numbers. For example, consider the numbers 30 ( $2 \times 3 \times 5$ ), 36 ( $2 \times 2 \times 3 \times 3$ ), 42 ( $2 \times 3 \times 7$ ), 45 ( $3 \times 3 \times 5$ ). 3 is the largest number that divides each of these numbers, and hence, is the HCF for these numbers.

**HCF is also known as Greatest Common Divisor (GCD).**

To find the HCF of two or more numbers, express each number as their prime factorization. The product of the minimum powers of common prime terms in both of the prime factorization gives the HCF. This is the method we illustrated in the above step.

Also, for finding the HCF of two numbers, we can also proceed by long division method. We divide the larger number by the smaller number (divisor). Now, we divide the divisor by the remainder obtained in the previous stage. We repeat the same procedure until we get zero as the remainder. At that stage, the last divisor would be the required HCF.

For example, HCF of 30 and 42:

The diagram illustrates the long division method for finding the HCF of 30 and 42. It shows a series of steps where the larger number is divided by the smaller number, and then the divisor is divided by the remainder. The remainders are 12, 6, and 0. The last non-zero remainder, 6, is circled and labeled as the HCF.

$$\begin{array}{r} 30 \overline{) 42} \quad 1 \\ \underline{- 30} \phantom{0} \\ 12 \quad 30 \quad 2 \\ \underline{- 24} \phantom{0} \\ 6 \quad 12 \quad 2 \\ \underline{- 12} \phantom{0} \\ 0 \end{array}$$

HCF

## Basic Euclidean Algorithm for HCF

The Euclidean algorithm is based on the below facts:

- If we subtract the smaller number from larger (we reduce larger number), GCD doesn't change. So if we keep subtracting repeatedly the larger of two, we end up with GCD.
- Now instead of subtraction, if we divide the smaller number, the algorithm stops when the remainder is found to be 0.

Below is the recursive function for finding GCD using Euclidean Algorithm:

```
gcd(a, b)
{
    if (a == 0)
        return b;

    return gcd(b % a, a);
}
```

**Time Complexity:**  $O(\log(\min(a, b)))$

**Important properties of LCM and HCF:**

1. For two numbers say, 'a' and 'b',  $LCM \times HCF = a \times b$ .
2. HCF of co-primes = 1.
3. For two fractions,
  - $HCF = HCF(\text{Numerators}) / LCM(\text{Denominators})$
  - $LCM = LCM(\text{Numerators}) / HCF(\text{Denominators})$

### Factorials

**Factorial:** In mathematics, the factorial of a number say **N** is denoted by **N!**. The factorial of a number is calculated by finding multiplication of all integers between 1 and N(both inclusive.)

For Example,  $4! = 4 * 3 * 2 * 1 = 24$ .

That is,

```
N! = N * (N-1) * (N-2) * . . . * 2 * 1
```

**Note:** As, per convention,  $0! = 1$ .

---

**Sample Problem:** Given a number N, the task is to count number of **trailing zeroes** in factorial of N. That is, number of zeroes at the end in the number **N!**.

**For Example:**



```
Input: N = 5
Output: 1
Factorial of 5 is 120 which has one trailing 0.

Input: N = 20
Output: 4
Factorial of 20 is 2432902008176640000 which has
4 trailing zeroes.
```

An efficient way to solve this problem is to observe the properties of prime factorization. Consider prime factors of **N!**. A trailing zero is always produced by the prime factors **2** and **5**. If we can count the number of 5s and 2s in prime factorization of N!, our task is done.

Consider the following examples:

- **N = 5:** There is one 5 and 3 2s in prime factors of 5! ( $2 * 2 * 2 * 3 * 5$ ). So count of trailing 0s is 1.
- **N = 11:** There are two 5s and three 2s in prime factors of 11! ( $2 * 8 * 34 * 52 * 7$ ). So count of trailing 0s is 2.

We can easily observe that the number of 2s in prime factors is always more than or equal to the number of 5s. So if we count 5s in prime factors, we are done.

Now, how to count total number of 5s in prime factors of N!? A simple way is to calculate  $\text{floor}(N/5)$ . For example, 7! has one 5, 10! has two 5s. It is not done yet, there is one more thing to consider. Numbers like 25, 125, etc have more than one 5. For example if we consider 28!, we get one extra 5 and number of 0s become 6. Handling this is simple, first divide N by 5 and remove all single 5s, then divide by 25 to remove extra 5s and so on. Following is the summarized formula for counting trailing 0s.

```
Trailing 0s in N! = Count of 5s in prime factors of n!
                  = floor(n/5) + floor(n/25) + floor(n/125) + ....
```

### Permutation and Combinations Basics

## Permutation

**Permutation** is the different arrangements of a given number of elements taken one by one, or some, or all at a time. For example, if we have two elements A and B, then there are two possible arrangements, AB and BA.

Number of permutations when 'r' elements are arranged out of a total of 'n' elements is  ${}^n P_r = \frac{n!}{(n-r)!}$ . For example, let  $n = 4$  (A, B, C and D) and  $r = 2$  (All permutations of size 2). The answer is  $4!/(4-2)! = 12$ . The twelve permutations are AB, AC, AD, BA, BC,

BD, CA, CB, CD, DA, DB and DC.

### Important Properties of Permutation:

1.  ${}^n P_n = n \cdot (n-1) \cdot (n-2) \cdot \dots \cdot 1 = n!$ .
2.  ${}^n P_0 = n! / n! = 1$ .
3.  ${}^n P_1 = n$ .
4.  ${}^n P_{n-1} = n!$ .
5.  ${}^n P_r / {}^n P_{r-1} = n - r + 1$ .

**Permutation with repetition allowed:** The number of permutation or arrangements of N numbers with repetition allowed will be  $N^n$ . For Example, permutations of {1,2} with repetitions will be {{1,1}, {1,2}, {2,1},{2,2}}.

**Permutation with duplicates:** The number of permutations or arrangements of N objects of which  $p_1$  are of one kind,  $p_2$  are of second kind, ...,  $p_k$  are of k-th kind and the rest if any, are of different kinds is:  $N! / (p_1! \cdot p_2! \cdot \dots \cdot p_k!)$ .

## Combination

**Combination** is the different selections of a given number of elements taken one by one, or some, or all at a time. For example, if we have two elements A and B, then there is only one way to select two items, we select both of them.

Number of combinations when 'r' elements are selected out of a total of 'n' elements is  ${}^n C_r = n! / [ (r!) \cdot (n - r)! ]$ . For example, let  $n = 4$  (A, B, C and D) and  $r = 2$  (All combinations of size 2). The answer is  $4! / ((4-2)! \cdot 2!) = 6$ . The six combinations are AB, AC, AD, BC, BD, CD.

### Important Properties of Combination:

1.  ${}^n C_0 = {}^n C_n = 1$ .
2.  ${}^n C_r = {}^n C_{n-r}$ .
3.  ${}^n C_r + {}^n C_{r-1} = {}^{n+1} C_r$ .
4.  $n \cdot {}^{n-1} C_{r-1} = (n - r + 1) \cdot {}^n C_{r-1}$ .

## Modular Arithmetic

Let us take a look at some of the **basic rules and properties** that can be applied in Modular Arithmetic(Addition, Subtraction, Multiplication etc.). Consider numbers **a** and **b** operated under modulo **M**.

1.  $(a + b) \bmod M = ((a \bmod M) + (b \bmod M)) \bmod M$ .
2.  $(a - b) \bmod M = ((a \bmod M) - (b \bmod M)) \bmod M$ .
3.  $(a * b) \bmod M = ((a \bmod M) * (b \bmod M)) \bmod M$ .

The above three expressions are valid and can be performed as stated. But when it comes to modular division, there are some limitations.

There isn't any formula to calculate:

$$(a / b) \bmod M$$

For this we have to learn **modular inverse**.

## Modular Inverse

The modular inverse is an integer 'x' such that.

$$a \cdot x \equiv 1 \pmod{M}$$

The value of x should be in  $\{0, 1, 2, \dots, M-1\}$ , i.e., in the ring of integer modulo M.

The multiplicative inverse of "a modulo M" exists if and only if a and M are relatively prime (i.e., if  $\gcd(a, M) = 1$ ).

### Examples:

**Input:** a = 3, M = 11

**Output:** 4

Since  $(4*3) \bmod 11 = 1$ , 4 is modulo inverse of 3

One might think, 15 also as a valid output as " $(15*3) \bmod 11$ " is also 1, but 15 is not in ring  $\{0, 1, 2, \dots, 10\}$ , so not valid.

**Input:** a = 10, M = 17

**Output:** 12

Since  $(10*12) \bmod 17 = 1$ , 12 is modulo inverse of 10

**Methods of finding Modular Inverse:** There are two very popular methods of finding

modular inverse of any number **a** under modulo **M**.

1. **Extended Euclidean Algorithm:** This method can be used when **a** and **M** are co-prime.
2. **Fermat Little Theorem:** This method can be used when **M** is prime.

Let us look at each of the above two methods in details:

**Extended Euclidean algorithm** that takes two integers 'a' and 'b', finds their gcd and also find 'x' and 'y' such that,

$$ax + by = \gcd(a, b)$$

To find modulo inverse of 'a' under 'M', we put  $b = M$  in the above formula. Since we know that a and M are relatively prime, we can put value of gcd as 1.

So, the formula becomes:

$$ax + My = 1$$

If we take modulo M on both sides, we get:

$$ax + My \equiv 1 \pmod{M}$$

We can remove the second term on left side, as ' $My \pmod{M}$ ' would always be 0 for an integer y.

Therefore,

$$ax \equiv 1 \pmod{M}$$

So the 'x' that we can find using [Extended Euclid Algorithm](#) is modulo inverse of 'a'.

**Fermat Little Theorem:** The Fermat's little theorem states that if M is a prime number, then for any integer a, the number  $a^M - a$  is an integer multiple of M.

That is,

$$a^M \equiv a \pmod{M}.$$

Since, a and M are co-prime to each other then  $a^{M-1}$  is an integral multiple of M. That is,

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

If we multiply both sides by  $a^{-1}$ , we get:

$$a^{-1} \equiv a^{M-2} \pmod{M}$$

Therefore, if **M** is a **prime number** to find modulo inverse of **a** under **M**, find **modular exponentiation of  $a^{M-2}$  under modulo M**.