Name: Sourashis Mondal

# MENU

1. Preliminaries
2. Divisibility theory in integers
3. Primes and their distn
4. Theory of Congruence [Excluding Linear Congruence and Chinese Remainder th.]

# NUMBER THEORY

## ① PRELIMINARIES :~

- **Well ordering Principle :-**
  Every non empty subset of $\mathbb{N}$ contains a least element.

  i.e, if $S$ be a non empty subset of $\mathbb{N}$, there is some natural number $a$ in $S$, s.t, $a \leq x \ \forall \ x \in S$

- **Archimedean property :** If $a$ and $b$ are positive integers, then, $\exists \ n \in \mathbb{N}$, s.t, $na \geq b$.

- **First Principle of Induction :-**
  Let, $S \subset \mathbb{N}$, s.t,
  (i) $1 \in S$
  and, (ii) whenever a natural number $k$ belongs to $S$, then $k+1$ also belongs to $S$.
  Then $S = \mathbb{N}$.

- Let, $E_n$ be a statement involving a natural number $n$,
  **Basis of Induction:** $E_1$ is true
  **Induction Step:** $E_{k+1}$ is true, whenever $E_k$ is true $\forall \ k \in \mathbb{N}$
  • The assumptions made in carrying out the induction step are known as induction hypotheses.

- **Second Principle of Induction :-**
  Let, $S \subset \mathbb{N}$, s.t;
  (i) $1 \in S$
  and, (ii) if $k$ is a +ve integer such that $1, 2, \cdots k$ belong to $S$, then $(k+1)$ must also be in $S$.
  or, if, $\{1, 2, \cdots k\} \subseteq S$, then $(k+1) \in S$
  Then, $S = \mathbb{N}$.

• **Lucas seq$^n$**: 1, 3, 4, 7, 11, 18, 29, 47, 76, .....

Basis : $a_1 = 1$ , $a_2 = 3$

Induction Step : $a_n = a_{n-1} + a_{n-2}$ , here, $a_n < \left(\frac{7}{4}\right)^n$

---

(*) $a^n - b^n = (a-b)(a^{n-1} + a^{n-2}\cdot b + a^{n-3}\cdot b^2 + \cdots$
$\cdots + a^2\cdot b^{n-3} + a\cdot b^{n-2} + b^{n-1})$

---

(*) The cube of any integer can be written as the difference of two squares

$\Rightarrow n^3 = (1^3 + 2^3 + 3^3 + \cdots + n^3) - (1^3 + 2^3 + \cdots + (n-1)^3)$

$= \left\{\frac{n(n+1)}{2}\right\}^2 - \left(\frac{(n-1)n}{2}\right)^2$

---

(*) Bernoulli inequality : If, $1+a > 0$, then,
$(1+a)^n \geq 1 + na$

---

Conjecture :- Mathematical statement, that has not been proved by anyone yet, but it can neither be disproved.

---

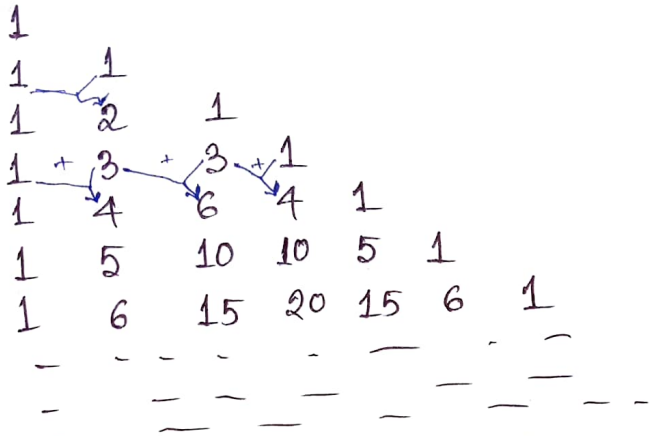
Collatz conjecture :-

$$T(n) = \begin{cases} \frac{n}{2}, & \text{if } n \text{ is even} \\ \frac{3n+1}{2}, & \text{if } n \text{ is odd} \end{cases}$$

The $3n+1$ conjecture is the claim that starting from any integer $n > 1$, the sequence of iterates $T(n)$, $T(T(n))$, $T(T(T(n)))$, ..... eventually reaches the integer 1 and subsequently runs through the values 1 and 2.

## Pascal's triangle:

in which, the binomial coeff. $^nC_k$ appears as $(k+1)^{th}$ number in the $n^{th}$ row.




All the boundary elements are 1, and, other elements are,

$$P_{ij} = P_{i-1,j-1} + P_{i-1,j}$$

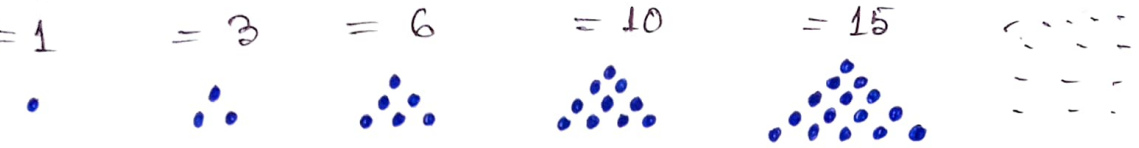
where
$i \rightarrow$ Row
$j \rightarrow$ Column

# DIVISIBILITY THEORY IN INTEGERS

## Triangular Number :~

Represents the number of dots, that can be arranged evenly in an equilateral triangle.

$1 = 1$ $\quad 1+2 = 3$ $\quad 1+2+3 = 6$ $\quad 1+2+3+4 = 10$ $\quad 1+2+3+4+5 = 15$



A number is called Triangular number, if it is the sum of consecutive integers, begining with 1.

(a) A number is triangular, if and only if, it is of the form $\frac{n(n+1)}{2}$

(b) The integer $n$ is a triangular number, if and only if, $8n+1$ is a perfect square

$\Rightarrow n = 1+2+\cdots+k = \frac{k.(k+1)}{2}$

Now, $8n+1 = 8 \times \frac{k(k+1)}{2} = 4k^2+4k+1 = (2k+1)^2$

(c) The sum of any two consecutive triangular numbers is a perfect square.

$\therefore t_n + t_{n-1} = n^2$

$\Rightarrow t_n + t_{n+1}$

$= (1+2+\cdots+n) + (1+2+\cdots+n+(n+1))$

$= \frac{n(n+1)}{2} + \frac{(n+1)(n+2)}{2} = \frac{n+1}{2}(2n+2) = (n+1)^2$

(d) If $n$ is a triangular number, then so are, $(9n+1)$, $(25n+1)$ and $(49n+6)$

$\Rightarrow 9n+1 = 9 \times \frac{k(k+1)}{2} + 1 = \frac{9k^2+9k+2}{2}$

$= \frac{9k^2+6k+3k+2}{2} = \frac{3k(3k+2)+(3k+2)}{2}$

$= \frac{(3k+1)((3k+1)+1)}{2} = \frac{m.(m+1)}{2}$

(e) $n$ $C_2$ represents the $(n-1)$ th

(e) $n+1 C_2$ represents the $n$ th triangular number.

$\left(\frac{n(n+1)}{2}\right)$

(4) $\{3(2k+1)\}^2$

$= 9(4k^2+4k+1)$

(f) • $t_k^2 - t_{k-1}^2 = k^3$

• $t_k + t_{k-1} = k^2$

(*) $t_1 + t_2 + t_3 + \cdots + t_n = \frac{n(n+1)(n+2)}{6}$

$\Rightarrow \sum_{i=1}^{n} t_i = \sum_{1}^{n} \frac{i(i+1)}{2} = \frac{n(n+1)(n+2)}{6}$

## Divison Algorithm :

Given integers $a$ and $b$, with $b > 0$, there exist unique integers $q$ and $r$, s.t,

$$a = bq + r \text{ , where, } 0 \leq r < b$$

---

**Th:** Given integers $a$ and $b$, with $b \neq 0$, $\exists$ unique integers $q$ and $r$, st, $a = bq + r$; where,

$$0 \leq r < |b|$$

---

**Th:**

(i) $a|0$, $1|a$, $a|a$

(ii) $a|1$ if and only if $a = \pm 1$

(iii) If, $a|b$ and $c|d$, then $ac|bd$.

(iv) If, $a|b$ and $b|c$, then $a|c$

(v) $a|b$ and $b|a \iff a = \pm b$

(vi) $a|b$ and, $b \neq 0 \Rightarrow |a| \leq |b|$

(vii) $a|b$, and $a|c \Rightarrow a|(bx + cy) \quad \forall\ x, y \in \mathbb{Z}$

---

**Linear Combination :** By a linear combination of $a$ and $b$, we mean an expression of the form $ax + by$, where, $x, y \in \mathbb{Z}$.

---

(*) The product of $m$ consecutive integers in divisible by $m$,

$$\forall\ c \in \mathbb{Z},$$
$$m \mid c \times (c+1) \times (c+2) \times \ldots \times (c + (m-1))$$

---

(*) The square of any odd number is of the form $8k + 1$.

$$\Rightarrow (2m+1)^2 = 4m^2 + 4m + 1$$
$$= 4m(m+1) + 1 = 4 \times 2k + 1 = 8k + 1$$

## GCD :-

Let a and b be given integers with at least one of them being non zero, the greatest common divisor of a and b, denoted by $\gcd(a,b)$ is the positive integer d, satisfying :

(i) $d|a$ and, $d|b$

(ii) if, $c|a$ and $c|b$, then $c \leq d$

---

**Alternate Condition :-** $d = \gcd(a,b)$, if, and only if,

(i) $d|a$ and $d|b$

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

---

**Theorem :-** • $\gcd(a,b)$ can be represented as a linear combination of a and b (but, it is not unique)

$$\gcd(a,b) = a.u + b.v \text{ , where, } u, v \in \mathbb{Z}$$

(*) The $\gcd(a,b)$ is the least positive value of $(ax+by)$, where $x, y \in \mathbb{Z}$.

- But, x, and y are not unique.

---

**Th :** If $K \in \mathbb{N}$, then, $\gcd(ka, kb) = |K| \times \gcd(a,b)$

---

**Th :** If, a and b are given integers, not both zero, then the set, $T = \{ax+by : x, y \in \mathbb{Z}\}$ is precisely the set of all multiples of $d = \gcd(a,b)$

i.e, you can represent all multiples of $d=\gcd(a,b)$ with the help of the linear combination of a and b (i.e. $ax+by$)

Eg: (i) $\gcd(3,6) = 3$

$\Rightarrow 3 = 6\times 1 - 3\times 1$

Now, $3K = (6\times 1 - 3\times 1)K$

∴ You can represent any $3K \in \mathbb{N}$, $\forall$ $K$

(ii) $\gcd(5,7) = 1$

$\Rightarrow 1 = 5\times 3 - 7\times 2$

$\Rightarrow K = K(5\times 3 - 7\times 2) = 5\times \underbrace{(3K)}_{x} + 7\times \underbrace{(-2K)}_{y}$

∴ You can represent any natural number with the help of $5\times(3K) + 7\times(-2K)$

---

**Relatively Prime / Coprime:**

Two integers $a$ and $b$, not both zero, are said to be relatively prime or, prime to each other, if, $\gcd(a,b) = 1$.

---

**Th:** $a$ and $b$ are prime to each other, if and only if, $\exists$ integers $u$ and $v$, s.t; $1 = au + bv$.

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

**Th:** If, $a \mid c$ and $b \mid c$, with $\gcd(a,b) = 1$, then $ab \mid c$

**Th:** $\gcd(a^n, b^n) = \{\gcd(a,b)\}^n$ (??)

**Th: Euclid's lemma:-** If, $a \mid bc$, with, $\gcd(a,b) = 1$, then $a \mid c$

**Th:** If, $a$ and $b$ are coprime, and $a$ and $c$ are coprime, then $a$ and $bc$ are coprime.

---

(*) If, $d = \gcd(a,b)$, then, $\gcd(a^n, b^n) = d^n$

(*) Two consecutive numbers are always coprime.

(8) Product of any five consecutive integers, is divisible by 5, 4, 3, 2.

Product of $n$ consecutive integers is divisible by $n!$
$\because {}^{m}C_n = \frac{m(m-1)(m-2)\cdots(m-n+1)}{n!} \times \frac{(m-n)!}{(m-n)!} = \text{integer}$

$\Rightarrow$ Let, ~~$m(m+1)(m+2)$~~

$P = m \times (m+1) \times (m+2) \times (m+3) \times (m+4)$

$\rightarrow$ It is divisible by 5, because product of five consecutive integers

$\rightarrow$ " " " " 4, " " " four " "

$\rightarrow$ " " " " 3, " " " three " "

Now, $\gcd(5,4) = 1$, $\therefore$ 5 and 4 are coprime.

~~P is divisible~~ $\therefore 5 \mid P$ and $4 \mid P \Rightarrow 5 \times 4 \mid P$

$\Rightarrow 20 \mid P$

also, 20 and 3 are coprime

$\therefore 20 \mid P$ and $3 \mid P \Rightarrow 3 \times 20 \mid P$

$\Rightarrow 60 \mid P$

---

(A) $a^n - b^n = (a-b)(a^{n-1} + a^{n-2}.b + a^{n-3}.b^2 + \cdots + ab^{n-2} + b^{n-1})$

for all $n$

(*) $a^n + b^n = (a+b)(a^{n-1} - a^{n-2}.b + a^{n-3}.b^2 - \cdots - a.b^{n-2} + b^{n-1})$

only if $n$ is odd

(*) $(1+2+3+\cdots+n) \mid (1^r + 2^r + 3^r + \cdots + n^r)$

for any odd number $r$.

# Euclidean Algorithm :~

"The number of steps required in the Euclidean Algorithm is at most (5 × number digits of smaller number)"

**Lemma :-** Assuming, $a > b$,

$\gcd(a, b) = \gcd(b, r)$, where, $a = bq + r$

**Proof :** Let, $d = \gcd(a, b)$ | $a = bq + r$

$\therefore d \mid a$ and $d \mid b$ ——— (i)

$\Rightarrow d \mid (a - bq)$

$\Rightarrow d \mid r$ ——— (ii)

from (i) and (ii), $d \mid b$ and $d \mid r$

$\therefore$ d is a common divisor of b and r.

Now, let, c is a common divisor of b and r.

$\therefore c \mid (bq + r) \Rightarrow c \mid a$

$\therefore c \mid a$ and, $c \mid b$, and we know d is the gcd of a and b.

$\therefore c \mid d$

$\therefore$ We have, $d \mid b$, $d \mid r$ and c is a common divisor of b and r, such that, $c \mid d$

$\therefore$ d is the gcd of b and r,

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

---

We utilize this lemma to find $\gcd(a, b)$ :

(i) Base case : $\gcd(r_n, 0) = r_n$

(ii) Recursive case : $\gcd(a, b) = \gcd(b, r)$

$\Rightarrow \therefore \gcd(a, b) = \gcd(b, r)$

$= \gcd(r_1, r_2)$

$= \gcd(r_n, 0) = r_n$

$a = bq + r$

$r = r_1 q_1 + r_2$

$r_1 = r_2 q_2 + r_3$

⋮

## Recursive Program to find gcd(a, b) using Euclid's Algorithm :—

```
int gcd (a, b)
{
    max = max (a, b);
    min = min (a, b);
    if (min == 0)
        return max;
    else
        return gcd (min, max % min);
}
```

Base case : $gcd(a, 0) = 0$

Recursive Case : $gcd(a, b) = gcd(b, a \% b)$ (assuming $a > b$)

---

(*) Prove, $a^n - b^n = (a-b)(a^{n-1} + a^{n-2}.b + \cdots + b^{n-1})$

$\Rightarrow 1 + \left(\frac{a}{b}\right) + \left(\frac{a}{b}\right)^2 + \cdots + \left(\frac{a}{b}\right)^{n-1}$

$= \frac{1.\{\left(\frac{a}{b}\right)^n - 1\}}{\frac{a}{b} - 1} = \frac{a^n - b^n}{a-b} \times \frac{b}{b^n}$

or, $a^n - b^n = (a-b) \times b^{n-1}\left(1 + \frac{a}{b} + \left(\frac{a}{b}\right)^2 + \cdots + \left(\frac{a}{b}\right)^{n-1}\right)$

$\therefore a^n - b^n = (a-b)(b^{n-1} + a.b^{n-2} + a^2.b^{n-3} + \cdots + a^{n-1})$

---

(*) Prove, $a^n + b^n = (a+b)(a^{n-1} - a^{n-2}.b + a^{n-3}.b^2 - \cdots + b^{n-1})$ if, $n$ is odd.

$\Rightarrow 1 + \left(-\frac{a}{b}\right) + \left(-\frac{a}{b}\right)^2 + \cdots + \left(-\frac{a}{b}\right)^{n-1}$

$= 1\frac{\{1 - \left(-\frac{a}{b}\right)^n\}}{1 - \left(-\frac{a}{b}\right)} = \frac{1 - \left(-\frac{a}{b}\right)^n}{1 + \frac{a}{b}}$

$= \frac{1 - (-1)^n.\frac{a^n}{b^n}}{1 + \frac{a}{b}} = \frac{b^n - (-1)^n.a^n}{b + a} \times \frac{b}{b^n}$

$$\text{or, } b^n - (-1)^n \cdot a^n = (b+a) \times b^{n-1}\left\{1 + \left(-\frac{a}{b}\right) + \left(-\frac{a}{b}\right)^2 + \cdots + \left(-\frac{a}{b}\right)^{n-1}\right\}$$

$$= (a+b)\left\{b^{n-1} + (-a)\cdot b^{n-2} + (-a)^2 \cdot b^{n-3} + \cdots + (-a)^{n-1}\right\}$$

If, $n$ = odd ;

$$b^n + a^n = (a+b)\left(b^{n-1} - ab^{n-2} + a^2 \cdot b^{n-3} - \cdots + a^{n-1}\right)$$

$$\text{or, } a^n + b^n = (a+b)\left(a^{n-1} - a^{n-2}\cdot b + a^{n-3}\cdot b^2 - \cdots + b^{n-1}\right)$$

---

(*) Prove that, $(a^d - b^d) \mid (a^n - b^n)$ if, $d \mid n$.

$$\Rightarrow a^n - b^n = a^{kd} - b^{kd} \quad \left[\because d \mid n \;\therefore \text{let, } n = kd\right]$$

$$= (a^d)^k - (b^d)^k$$

$$= (a^d - b^d)\left\{(a^d)^{k-1} + (a^d)^{k-2}\cdot(b^d) + \cdots + (b^d)^{k-1}\right\}$$

$$\therefore (a^d - b^d) \mid (a^n - b^n) \quad \text{if, } d \mid n.$$

Eg: $15 \mid (2^{4n} - 1)$

$\because (2^4 - 1) \mid (2^{4n} - 1)$ and, $4 \mid 4n$

---

(*) The sum of squares of two odd integers cannot be a perfect square.

$$\Rightarrow (2m+1)^2 + (2n+1)^2$$

$$= 4m^2 + 4m + 1 + 4n^2 + 4n + 1$$

$$= 2\underbrace{(2m^2 + 2n^2 + 2m + 2n + 1)}_{\text{Odd number}}$$

2 is not a factor of $(2m^2 + 2n^2 + 2m + 2n + 1)$.

That means, 2 doesn't have a pair in the factors of $(2m+1)^2 + (2n+1)^2$.

$\therefore$ So, $(2m+1)^2 + (2n+1)^2$ can't be perfect square.

(*) The product of four consecutive natural number + 1 is perfect square.

$$\Rightarrow a(a+1)(a+2)(a+3) + 1$$
$$= (a+1)(a+2) \times a(a+3) + 1$$
$$= (a^2+3a+2)(a^2+3a) + 1$$
$$= (a^2+3a)^2 + 2.(a^2+3a).1 + 1^2$$
$$= (a^2+3a+1)^2$$

---

(*) Difference of two consecutive cubes is always Odd.

$$\Rightarrow (a+1)^3 - a^3$$
$$= (a+1-a)\{(a+1)^2 + (a+1).a + a^2\}$$
$$= a^2+2a+1+a^2+a+a^2$$
$$= 3a^2+3a+1$$
$$= 3a(a+1) + 1$$
$$= 3 \times 2m + 1 \quad [\because a(a+1) = \text{Even} = 2m \text{ (say)}]$$
$$= 6m + 1$$
$$= \text{Even} + 1 = \text{Odd}$$

if, $a$ = Even,
then, $(a+1)^3 - a^3$
$\equiv (0+1)^3 - 0^3 \pmod 2$
$\equiv 1 \pmod 2$

if $a$ = odd,
then, $(a+1)^3 - a^3$
$\equiv (1+1)^3 - 1^3 \equiv -1 \equiv 1 \pmod 2$

---

(*) $\gcd(a, a+n) \mid n$

$\Rightarrow$ let, $\gcd(a, a+n) = d$

$\therefore d \mid$ Any linear combination of $a$, and $(a+n)$

or, $d \mid (a+n) + (-1).a$

or, $d \mid n$

$\therefore \gcd(a, a+n) \mid n$

Corollary: $\gcd(a, a+1) = 1$.

(*) If, $\gcd(a,b) = ax + by$, then prove that $x$ and $y$ are coprime.

$\Rightarrow$ $\gcd(a,b) = d$

$\therefore$ $d = ax + by$

or, $1 = \left(\frac{a}{d}\right)x + \left(\frac{b}{d}\right)y$

or, $1 = x \times m + y \times n$ $\left[\because d = \gcd(a,b), \therefore d|a \text{ and } d|b\right]$

$\therefore$ $\gcd(x, y) = 1$

---

(*) Prove that $\gcd(5a+2, 7a+3) = 1$

$\Rightarrow$ Let, $\gcd = d$

$\therefore d \mid |7 \times (5a+2) - 5(7a+3)|$ [we are eliminating $a$]

or, $d \mid |14 - 15|$

or, $d \mid 1$

$\therefore d = 1$

---

(*) ~~$\gcd(a,b) = \gcd(ax+by, au+bv)$~~ ? ?

---

(*) Prove than, $\frac{(3n)!}{(3!)^n}$ is an integer $\forall\ n \geq 0$

$\Rightarrow$ ~~$(3n)!$~~ we need to prove,

$(3!)^n \mid (3n)!$

i.e, $2^n \cdot 3^n \mid (3n)!$

Now, $(3n)! = 1.2.3.4.5.6 \ldots\ldots 3n$

$= \{3.6.9.12 \ldots (3n-3).3n\} \times \{1.2.4.5.7.8.10 \ldots \ldots (3n-1)$

$= 3^n \{1.2.3.4 \ldots (n-1).n\} \times \{1.2.4.5.7.8 \ldots (3n-1$

$\therefore 3^n \mid (3n)!$ ——— (i)

(A)(*) Prove that $\frac{(3n)!}{(3!)^n}$ is an integer $\forall\ n \geq 0$

$\Rightarrow$ ~~We can represent~~

$$(3n)! = 1.2.3.\cdots 3n = \prod_{k=1}^{3n} (k)$$

$3! = 2 \times 3$

We can represent any number $k$ as, $k = qi + r$,

where, $0 \leq r < q$

Now, To find the factors of 3's multiple in $(3n)!$,

We take, $q = 3$

$$\therefore (3n)! = \prod_{i=1}^{3n} k = 1.2.3.4.5.6.7.\cdots (3n-2).(3n-1).3n$$

$$= \prod_{i=1}^{n} (3i) \times \prod_{i=0}^{n-1} (3i+1) \times \prod_{i=0}^{n-1} (3i+2)$$

$$= 3^n \times \prod_{i=1}^{n} i \times \prod_{i=0}^{n-1} (3i+1) \times \prod_{i=0}^{n-1} (3i+2)$$

$$\therefore 3^n \mid (3n)! \quad \text{---------- (i)}$$

Again, to find the factors of 2's multiple in $(3n)!$,

we take, $q = 2$

$$\therefore (3n)! = \begin{cases} \prod_{i=1}^{\frac{3n}{2}} (2i) \times \prod_{i=0}^{\frac{3n-2}{2}} (2i+1), & \text{if } (3n) = \text{Even} \\ \prod_{i=1}^{\frac{3n-1}{2}} (2i) \times \prod_{i=0}^{\frac{3n-1}{2}} (2i+1), & \text{if } (3n) = \text{odd} \end{cases}$$

$3n = 2m$, $m = \frac{3n}{2}$

and, $3n-1 = 2m$, $m = \frac{3n-1}{2}$

$3n = 2m+1$, $m = \frac{3n-1}{2}$

and, $3n+1 = 2m$, $m = \frac{3n-1}{2}$

$$= \begin{cases} \left\{ \prod_{i=1}^{n} (2i) \times \prod_{i=n+1}^{3n/2} (2i) \right\} \times \prod_{i=0}^{\frac{3n-2}{2}} (2i+1) & , \text{if } (3n) = \text{even} \\ \left\{ \prod_{i=1}^{n} (2i) \times \prod_{i=n+1}^{\frac{3n-1}{2}} (2i) \right\} \times \prod_{i=0}^{\frac{3n-1}{2}} (2i+1) & , \text{if } (3n) = \text{odd} \end{cases}$$

$$= \begin{cases} 2^n \times n! \times \prod_{n+1}^{3n/2} 2i \times \prod_{0}^{\frac{3n-2}{2}} (2i+1), & \text{if } 3n = \text{even} \\ 2^n \times n! \times \prod_{i=n+1}^{\frac{3n-1}{2}} 2i \times \prod_{0}^{\frac{3n-1}{2}} (2i+1), & \text{if } 3n = \text{odd} \end{cases}$$

$\therefore 2^n \mid (3n)!$ ——————— (ii)

from (i) and (ii) $2^n \mid (3n)!$ and, $3^n \mid (3n)!$

Now, 2 and 3 are coprime.

$\Rightarrow 2^n$ and $3^n$ are coprime.

$$\gcd(2^n, 3^n) = [\gcd(2,3)]^n = 1^n = 1$$

$\therefore 2^n \mid (3n)!$ and, $3^n \mid (3n)!$ and, $2^n$ and $3^n$ are coprime

$\therefore 2^n \times 3^n \mid (3n)!$

$\Rightarrow (3!)^n \mid (3n)!$

(*) Prove that, $\gcd(a^n, b^n) = \{\gcd(a,b)\}^n$

→ If, $n = 1$, $\gcd(a^n, b^n) = \gcd(a,b)$

Now, say, $\gcd(a^k, b^k) = [\gcd(a,b)]^k = [d]^k$

$\therefore d \mid x.a^k + y.b^k \quad \forall \quad x, y \in \mathbb{Z}$

---

(*) The product of consecutive $n$ integers is divisible by $n!$.

⇒ Let, the first integer be $(a+1)$.

$\therefore (a+1)(a+2)(a+3)\ldots(a+n)$

$= \frac{(a+n)!}{a!} = \frac{(a+n)!}{a! \times n!} \times n! = {}^{(a+n)}C_n \times n!$

$\therefore n! \mid (a+1)(a+2)\ldots(a+n)$.

(*) If, $\gcd(a,b) = 1$ and $\gcd(a,c) = 1$, then prove $\gcd(a, bc) = 1$

$\Rightarrow \quad 1 = ax + by$ for some $x, y, u, v$

and, $1 = au + cv$

$\therefore 1 = 1 \times 1 = (ax + by)(au + cv)$

~~$= ax(au + \ldots$~~

$= ax(au + cv) + by.au + bc\,xy$

or, $1 = a\{x(au + cv) + byu\} + bc \times (xy)$

or, $1 = a \times m + bc\,n$, for some $m$ and $n$

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

---

(*) If $\gcd(a,b) = 1$, then $\gcd(ac, b) = \gcd(c, b)$

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

$\Rightarrow ax + by = 1$ for some $x, y$

Now, $\gcd(ac, b) = d$ (Say)

$\Rightarrow ac \times u + b \times v = d$ for some $u, v$

$\Rightarrow c \times (au) + b \times (v) = d$

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

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

(#) If $\gcd(a,b) = 1$, and $c \mid (a+b)$,

then $\gcd(a,c) = \gcd(b,c) = 1$

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

$\Rightarrow ax + by = 1$ for some $x, y$ — (i)

Now, $c \mid (a+b)$

$\Rightarrow a + b = c \times k$ for some $k$

$\Rightarrow ay + by = cky$

$\Rightarrow ay + (1 - ax) = cky$ [From (i)]

$\Rightarrow a(x-y) + c(ky) = 1$

$\Rightarrow au + cv = 1$, $\begin{bmatrix} u = x - y \\ v = ky \end{bmatrix}$

$\rightarrow$ for some $u, v$

$\therefore \gcd(a,c) = 1$ (Proved)

Alternative: —

Let, $\gcd(a,c) = d$

$\therefore d \mid a$ and $d \mid c$

$\Rightarrow d \mid c - a$

$\Rightarrow d \mid (a+b-a)$

$\Rightarrow d \mid b$

Now, $\because \gcd(a,b) = 1$

and, $d \mid a$ and $d \mid b$

$\Rightarrow d \mid \gcd(a,b)$

$\Rightarrow d \mid 1$

$\Rightarrow d = 1$

$\Rightarrow \gcd(a,c) = 1$ (Proved)

(*) If, $\gcd(a,b) = 1$, $d \mid ac$ and, $d \mid bc$, then prove, $d \mid c$

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

$\Rightarrow ax + by = 1$ for some $x$ and $y$

$\Rightarrow acx + bcy = c$

$\Rightarrow mdx + ndy = c$ [$\because d \mid ac$ and $d \mid bc$, let, $ac = md$, $bc = nd$]

$\Rightarrow d(mx + ny) = c$

$\Rightarrow d \mid c$

---

## Important Property ||:-

(*) If, $d = \gcd(a,b)$, then $d \mid$ Any linear combination of $a, b$

$d = \gcd(a,b)$ is the least value of the linear combination of $a$ and $b$

$\Rightarrow d \mid (ax + by) \quad \forall \quad x, y \in \mathbb{Z}$

(*) If, $d \mid (ax + by)$ for some $x$ and $y$, we can't say that $d = \gcd(a,b)$, but if $d \mid a$ and $d \mid b$, then $d \mid (ax + by) \ \forall \ x, y \in \mathbb{Z}$ and $d \mid \gcd(a,b)$

## Application :-

(i) Prove that $\gcd(2a+1, 9a+4) = 1$

$\Rightarrow$ let, $d = \gcd(2a+1, 9a+4)$

$\Rightarrow d \mid (2a+1)x + (9a+4)y \quad \forall \quad x, y \in \mathbb{Z}$

$\Rightarrow d \mid 9(2a+1) - 2(9a+4)$ [taking, $x = 9$, $y = -2$]

$\Rightarrow d \mid 1$

$\Rightarrow d = 1$ (Proved)

(ii) Proove that, $\gcd(5a+2, 7a+3) = 1$

⇒ Let, $d = \gcd(5a+2, 7a+3)$

$\Rightarrow d \mid (5a+2)x + (7a+3)y \quad \forall \quad x, y \in \mathbb{Z}$

$\Rightarrow d \mid 7(5a+2) - 5(7a+3)$ [Eliminating a]

$\Rightarrow d \mid (14 - 15)$

$\Rightarrow d \mid -1 \Rightarrow d \mid 1 \Rightarrow d = 1$

---

(iii) If, a is odd, then, $\gcd(3a, 3a+2) = 1$

⇒ Let, $d = \gcd(3a, 3a+2)$

$\Rightarrow d \mid (3a+2) - 3a$

$\Rightarrow d \mid 2 \Rightarrow d = 1, \text{ or } 2$

Now, if a is odd,

then, $3a$ is odd

then, 2 cannot be a divisor of $3a$

$\therefore d = 1$ (Proved)

---

(iii) Proove that, $\gcd(2a-3b, 4a-5b)$ divides $b$.

Hence, $\gcd(2a+3, 4a+5) = 1$

⇒ 1st Part :-

Let, $d = \gcd(2a-3b, 4a-5b)$

$\Rightarrow d \mid 2(2a-3b) - (4a-5b)$ (Eliminating a)

$\Rightarrow d \mid b$ (Proved)

2nd Part :-

Let, $d = \gcd(2a+3, 4a+5)$

$\Rightarrow d \mid 2(2a+3)$ Here, $b = -1$

$\therefore d \mid (-1) \Rightarrow d \mid 1 \Rightarrow d = 1$ (Proved)

(*) Prove that $2^{35} - 1$ is divisible by 31 an 127.

⇒ It is an application of,
if $d|n$, then, $a^d - b^d \mid a^n - b^n$

Now, $2^{35} - 1$

$= (2^5)^7 - 1$

$= (32)^7 - (1)^7$

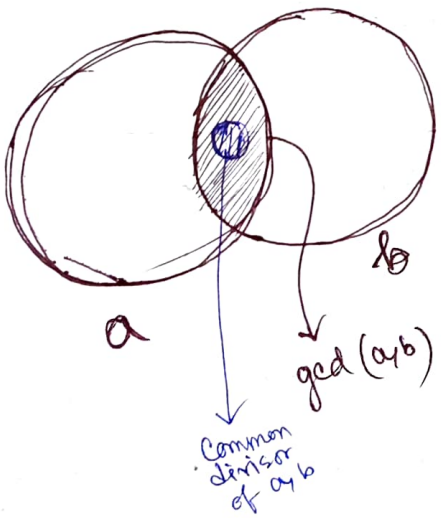
$= (32-1)\{(32)^{7-1} + (32)^{7-2} + (32)^{7-3} + \cdots + 32 + 1\}$

$= 31 \times \{\cdots\cdots\}$

$\therefore 31 \mid 2^{35} - 1$ (Ans)

---

(*) Q. K. Q.



## Least common Multiple :~

$m$ is the $lcm(a,b)$ if,

(i) $a|m$ and $b|m$

and, (ii) if, $a|c$ and $b|c$, with $c>0$, then, $m|c$ (or, $m \leq c$)

**Th:** $lcm(a,b) \times gcd(a,b) = ab$

Corollary: $lcm(a,b) = ab$, if and only if, $a$ and $b$ are coprime

- $gcd(a,b,c) = gcd(a, gcd(b,c))$

## Diophantine Equation :~

An equation in one or more unknowns which is to be solved in integers is said to be Diophantine equation.

**Th:** A linear Diophantine eqn $ax+by=c$ has a soln if and only if $d|c$, where $d = gcd(a,b)$.

If, $x_0$ and $y_0$ be any particular soln of this equation, then all other soln's are of the form $\left(x_0 + \left(\frac{b}{d}\right)t,\ y_0 - \left(\frac{a}{d}\right)t\right)$.

**Proof:** Let other soln be $(x,y)$.

$\therefore ax_0 + by_0 = c = ax + by$

or, $a(x-x_0) = b(y_0-y)$ ——— (i)

Now, $\because d = gcd(a,b)$,

$\therefore a = dr$ and, $b = ds$, where $r$ and $s$ are coprime.

$\left[\because gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1\right]$

$$r(x - x_0) = s(y_0 - y) \quad \text{---------- (ii)}$$

Now, $r \mid s(y_0 - y)$ and, $\gcd(r, s) = 1$

Using Euclid's lemma,

$$r \mid (y_0 - y)$$

Say, $y_0 - y = rt$, or, $y = y_0 - rt$

From (ii), $r(x - x_0) = rt \times s$

or, $x = x_0 + st$

$\therefore$ $\boxed{\begin{aligned} x &= x_0 + \left(\frac{b}{d}\right)t \\ \text{and } y &= y_0 - \left(\frac{a}{d}\right)t \end{aligned}}$ general sol$^n$

It is easy to see that, regardless of the choice of $t$, $(x, y)$ satisfies the eq$^n$

$$\text{LHS} = ax + by = a\left(x_0 + \frac{b}{d}t\right) + b\left(y_0 - \frac{a}{d}t\right)$$

$$= ax_0 + by_0 + \frac{ab}{d}t - \frac{ab}{d}t$$

$$= ax_0 + by_0$$

$$= c = \text{RHS}.$$

---

Important points :

(i) If we take, $x = x_0 + bt$, and, $y = y_0 - at$, we will get a sol$^n$ set, but we may not get every sol$^n$s.

(ii) If we take, $x = x_0 + \frac{b}{n}t$, $y = y_0 - \frac{a}{n}t$, then, $\frac{b}{n}$ and $\frac{a}{n}$ may not be integer, or we may not get every sol$^n$s.

**Corollary :-**

If $a$ and $b$ are coprime, then,

$$(x, y) = (x_0 + bt, y_0 - at)$$

---

(*) A famous linear indeterminate problem → "hundred fowls".

If a cock is worth 5 coins, a hen 3 coins, and three chicks together 1 coin, how many cocks, hens and chickens, totaling 100, can be bought for 100 coins.

⇒ Let, no. of cocks = $x$
" " hens = $y$
" " chicks = $z$

$\therefore 5x + 3y + \frac{1}{3}z = 100$ ——— (i) and, $x + y + z = 100$ ——— (ii)

or, $15x + 9y + z = 300$

or, $14x + 8y = 200$ [From (ii)]

or, $7x + 4y = 100$ ——— (iii)

Now, $\gcd(4, 7) = 1$

$\therefore$ (iii) has integer sol$^n$s.

Now, $1 = 7 \times (-1) + 4 \times (2)$

$\therefore x_0 = -1, y_0 = 2$

or, $100 = 7 \times (-100) + 4 \times (200)$

$\therefore x_0 = -100$ and, $y_0 = 200$

$$\therefore x = -100 + 4t, \quad y = 200 - 7t$$
$$\therefore z = 100 - x - y = 3t$$

——— (iv)

Now, $x, y, z \geq 0$

$\therefore$ $x \geq 0$ | $y \geq 0$ | $z \geq 0$

$\Rightarrow t \geq 25$ | $\Rightarrow t \leq 28\frac{4}{7}$ | $\forall\, t \geq 0$

$\text{or, } t \leq 28$

$\therefore t \in \{25, 26, 27, 28\}$

If $t = 25$, then $(x, y, z) = (0, 25, 75)$

If $t = 26$, then $(x, y, z) = (4, 18, 78)$

If, $t = 27$, then $(x, y, z) = (8, 11, 81)$

If $t = 28$, then, $(x, y, z) = (12, 4, 84)$

} Ans)

# Prime Numbers

**Definition :-**

An integer $p > 1$ is called a prime number, if its only positive divisors are 1 and $p$.

Other numbers $> 1$ are composites.

(*) 1 is neither a prime or composite number.

(*) 2 is the only even prime.

**Th:** If $p$ is a prime and $p \mid ab$, then $p \mid a$ or $p \mid b$.

**Corollary 1:** If $p$ is a prime and, $p \mid a_1 a_2 a_3 \cdots a_n$, then $p \mid a_k$ for some $k$ $[1 \le k \le n]$

**Corollary 2:** If $p, q_1, q_2, \cdots q_n$ are all primes and $p \mid q_1 q_2 q_3 \cdots q_n$, then, $p = q_k$ for some $k$.

## Fundamental theorem of Arithmetic :-

Every positive integer $n > 1$ is either a prime or a product of primes; this representation is unique, apart from the order, in which the factor occurs.

**Corollary :-**

Any positive integer $n > 1$ can be written uniquely in a canonical form.

$$n = p_1^{k_1} \cdot p_2^{k_2} \cdot p_3^{k_3} \cdots p_r^{k_r}$$

Each $k_i$ is a positive integer and each $p_i$ is a prime, with, $p_1 < p_2 < \cdots < p_r$

GCD can be determined with the help of unique prime factorization:

$$a = p_1^{k_1} \cdot p_2^{k_2} \cdots p_n^{k_n}$$

and, $b = p_1^{j_1} \cdot p_2^{j_2} \cdots p_n^{j_n}$

$\therefore \gcd(a,b) = p_1^{\gamma_1} \cdot p_2^{\gamma_2} \cdots p_n^{\gamma_n}$,

where, $\gamma_i = \min(k_i, j_i)$

## GCD and LCM

We can represent GCD and LCM also with help of prime factors.

Say, a and b are two numbers,

$$a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \cdots p_n^{\alpha_n} = \prod_i p_i^{\alpha_i}$$ { $p_i$ is prime number

$$b = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdots p_n^{\beta_n} = \prod_i p_i^{\beta_i}$$

Now,

(i) $\gcd(a,b) = p_1^{\gamma_1} \cdot p_2^{\gamma_2} \cdots p_n^{\gamma_n} = \prod_i p_i^{\gamma_i}$,

where, $\gamma_i = \min(\alpha_i, \beta_i)$

(ii) $\text{lcm}(a,b) = p_1^{\delta_1} \cdot p_2^{\delta_2} \cdots p_n^{\delta_n} = \prod_i p_i^{\delta_i}$

where, $\delta_i = \max(\alpha_i, \beta_i)$

**Lemma** :-

(i) $\min\{\alpha, \max\{\beta, \gamma\}\} = \max\{\min(\alpha,\beta), \min(\alpha,\gamma)\}$

(ii) $\max\{\alpha, \min(\beta, \gamma)\} = \min\{\max(\alpha,\beta), \max(\alpha,\gamma)\}$

**Th:** (i) $\gcd(a, \text{lcm}(b,c)) = \text{lcm}(\gcd(a,b), \gcd(a,c))$

(ii) $\text{lcm}(a, \gcd(b,c)) = \gcd(\text{lcm}(a,b), \text{lcm}(a,c))$

**Note:-**
gcd() and lcm are binary operations.
say, we define '$\circ$' and '$*$' s.t,

$a \circ b = \gcd(a,b)$

$a * b = \text{lcm}(a,b)$

$\therefore$ (i) $a \circ (b * c) = (a \circ b) * (a \circ c)$

(ii) $a * (b \circ c) = (a * b) \circ (a * c)$

$\Longrightarrow$ (*) '$\circ$' and '$*$' follow distributive property...

---

## Test for Primality :~

A composite number $n$ will always possess a prime divisor $p$, satisfying $p \leq \sqrt{n}$.

If a number $n$ doesn't have a prime factor $p \leq \sqrt{n}$, then, $n$ is a prime number.

**Proof:** Suppose, $a$ is a composite number, and $a > 1$,
then $a$ can be written as, $a = bc$,
where, $1 < b < a$ and $1 < c < a$.

Suppose, $b \leq c$

then, $b^2 \leq c \cdot b = a$ $\therefore$ $b^2 \leq a$

Because of Fundamental theorem of arithmetic, $b$ has at least one prime factor $p$.

$\therefore p \mid b$ and $b \mid a$

$\Rightarrow p \mid a$ and $p \leq b \leq \sqrt{a}$ or, $p \leq \sqrt{a}$

$\therefore$ If $a$ is a composite number, then it must contain a prime $\leq \sqrt{a}$.

# Sieve of Eratosthenes :-

This a technique for finding all prime numbers below a given integer $n$.

The scheme calls for writing down the integers from 2 to $n$ in their natural order and then systematically eliminating all the composite numbers by striking out all multiples $2p, 3p, 4p, 5p \ldots\ldots$ of the primes $p \leq n$. The integers that are left on the list, those that do not fall through the "sieve" are primes.

## Algorithm :-

1) Create a list of consecutive integers from 2 to $n$: (2, 3, 4, .... $n$)

2) Initially, let $p$ equal 2, the first prime

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.

4) 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.

## Implementation :-

```
// Create a Boolean array "prime[0.....n]" and
// initialize all entries of it as true. A value in
// prime[i] will finally be false if 'i' is not a
// prime, else true.

void SieveOfEratosthenes (int n)
{
    Bool prime[n+1];
    for (i=0; i<n+1; i++)
        prime[i] = true;

    for (int p=2; p*p<=n; p++)
    {
        // If prime[p] is not marked, then it is a prime
        if (prime[p] == true)
        {
            // Update all multiples of p greater than
            // or equal to the square of it.
            // Because numbers, which are multiple
            // of p and are less than p^2 are already
            // been marked as the multiple of
            // previous prime.

            for (int i= p*p; i<=n; i+=p)
                prime[i] = false;
        }
    }

    // print all primes
    for (int p=2; p<=n; p++)
        if (prime[p] == true)
            printf ("%d ", p);
}
```

We are considering the multiples of primes upto $\sqrt{n}$, because if n is a composite number, then n is the multiple of a prime, which is less than $\sqrt{n}$. That means that n will be eliminated from the prime number list, when the multiples of prime $p \le \sqrt{n}$ were being eliminated.

We are considering the multiples of p, starting from $p^2$, because other multiples $< p^2$, have already been eliminated from prime list while considering the multiples of the previous numbers less than p.

## Th. (Euclid) :-

The number of primes is infinite.

**Proof :**

Suppose, the number of primes in finite and let $p_n$ be the greatest prime.

and the other primes are, $p_1 = 2, p_2 = 3, p_3 = 5 \ldots$

Now, let,

$$N = p_1 p_2 p_3 \cdots p_n + 1$$

Now, $p_1 p_2 p_3 \cdots p_n$ is divisible by each of the primes $p_1, p_2, p_3 \cdots p_n$

So, $(p_1 p_2 p_3 \cdots p_n + 1)$ is not divisible by $p_1, p_2, p_3 \cdots p_n$

But, according to the Fundamental Th. of Arithmetic, there exists a prime number $p$, that divides $N$.

Hence, this number $N$ is either itself a prime number, or being a composite number, is divisible by a prime number greater than $p_n$. In Both cases $p_n$ fails to be the greatest prime.

Therefore the number of primes is infinite.

---

## Euclidean number :-

For a prime $p$, define $p^{\#}$ to be the product of all primes that are less than or equal to $p$.

Numbers of the form $(p^{\#} + 1)$ are called Euclidean numbers.

- The first 5 Euclidean numbers are primes.

eg: $2^{\#} + 1 = 3$, $7^{\#} + 1 = 211$

## Joseph Bertrand's Conjecture

### Some inequality :~

[$p_n$ = $n$th prime]

(i) Bonse's inequality :- $p_n^2 < p_1 p_2 \cdots p_{(n-1)}$

(ii) $p_{2n} \leq p_2 \cdot p_3 \cdot p_4 \cdots p_n - 2, \quad n \geq 3$

(iii) Theorem: $p_n \leq 2^{2^{n-1}}$

Corollary: For $n \geq 1$, there are atleast $(n+1)$ primes less than $2^{2^n}$.

(iv) Bertrand's Conjecture:-

Between $n \geq 2$ and $2n$, there is atleast one prime, i.e, $p_{n+1} < 2p_n$.

(v) $p_n < 2^n, \quad n \geq 2$

---

**Repunit:** A repunit is an integer written (in decimal) as a string of 1's, such as 11, 111, 1111, ....

We use the symbol $R_n$ to denote the repunit consisting of $n$ consecutive 1's.

$$R_n = \frac{10^n - 1}{9}$$

$\therefore R_2 = 11, \quad R_3 = 111 \ldots$

---

(*) Given any positive integer $n$, there exists $n$ consecutive composite numbers.

$\Rightarrow (n+1)! + 2, \quad (n+1)! + 3, \quad (n+1)! + 4, \ldots, (n+1)! + (n+1)$ are $n$ consecutive composite numbers.

Because, $(n+1)! + r$ is always divisible by $r$, if $2 \leq r \leq n+1$

eg: 4 consecutive composite numbers are:

$5! + 2 = 122 = 2 \times 61$

$5! + 3 = 123 = 3 \times 41$

$5! + 4 = 124 = 4 \times 31$

$5! + 5 = 125 = 5 \times 25$

## Goldbach's conjecture :-

Every even integer is the sum of two numbers that are either primes or 1.

A somewhat general formulation is that :
Every even integer greater that 4 can be written as a sum of two odd prime numbers,

eg: $9 = 2 + 7$

---

## $\pi$ ( ) :-

The number of primes less than a positive integer $x$ is denoted by $\pi(x)$.

$\pi_{a,b}(x)$ counts the number of primes of the form, $p = an + b$, not exceeding $x$.

---

**Lemma:** The product of two or more integers of the form $4n+1$ is of the same form

$$\Rightarrow (4n+1)(4m+1)$$
$$= 16mn + 4n + 4m + 1$$
$$= 4(4mn + n + m) + 1 = 4K + 1$$

---

(*) According to divison algorithm, all integers can be represented as $4n, 4n+1, 4n+2, 4n+3$
All the odd numbers are of the form $(4n+1)$ or $(4n+3)$.

**Th:** There are infinite number of primes of the form $(4n+3)$

**Th: Dirichlet :‖:–**

If, a and b are coprime positive integers, then, the arithmetic progression,

$a,\ a+b,\ a+2b,\ a+3b,\ \ldots\ldots$

contains infinitely many primes

---

(9) If, $2^n - 1$ be a prime, prove that $n$ is a prime.

⇒ Suppose, $n$ is composite.

Say, $n = p \cdot q$, where, $p, q > 1$

Now, $2^n - 1 = (2^p)^q - (1)^q$

$= (2^p - 1)\{(2^p)^{q-1} + (2^p)^{q-2} + \cdots + 2 + 1\}$

Each factor on the right is evidently greater than 1 $[\because p, q > 1]$, so $2^n - 1$ is composite.

Contrapositively, $(2^n - 1)$ is a prime number, if $n$ is prime.

---

(*) **Square free :–**

An integer is said to be square free, if no $\alpha_i$ in the canonical form of $n$ is greater than 1.

$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots\ p_n^{\alpha_n}$

eg: $3150 = 2 \cdot 3^2 \cdot 5^2 \cdot 7 \longrightarrow$ Not square free

$210 = 2 \cdot 3 \cdot 5 \cdot 7 \longrightarrow$ Square free

(*) Actually a square free integer is a number, which is not divisible by any perfect square, i.e, no prime factor divides it more than once.

## Program to check if a number is square-free or not :

We one by one find all prime factors. For every prime factor, we check if its square also divides n. If yes, then we return false. Finally if we do not find any prime factor, which divides it more than once, we return false.

```
Bool isSquareFree (int n)
{
    if (n % 2 == 0)
        n = n/2;

    // If 2 again divides n, then
    // n is not square free
    if (n % 2 == 0)
        return false;

    // n must be odd at this point, so we can
    // skip one element, and we check by dividing
    // with odd numbers twice. (We are ~~checking~~
    // using odd numbers instead of primes, because
    // all primes > 2 are odd and it will be hard
    // to find the primes. So we use odd numbers to
    // check.
    ~~odd~~.
    for (int i = 3; i <= sqrt(n); i += 2)
    {
        // check if i is a factor
        if (n % i == 0)
        {
            n = n/i;

            // If, i again divides n, then n
            // is not square free
            if (n % i == 0)
                return false;
        }
    }
    return true;
}
```

## Perfect Square :-

A number is a perfect square, if all its prime factors have even power. , i.e, $\alpha_i$ = even

eg : $144 = 2^4 \times 3^2$

Q. If $(2^n + 1)$ is an odd prime, prove that $n$ is a power of 2.

$\Rightarrow$ If, $n$ is odd, then, $(2^n + 1)$ is divisible by $(2+1)$

[ $\because 2^n + 1 = (2+1)(2^{n-1} - 2^{n-2} + 2^{n-3} \cdots - 2 + 1)$ if $n$ is odd ]

Then, it would be a composite number.

So, $n$ can not be odd.

$n$ is even.

Let, $n = 2^k \cdot p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_n^{\alpha_n}$, $p_i$ = Prime

or, $n = 2^k \times p$, $p$ = odd integer

If, $p > 1$, then,

$2^n + 1 = (2^{2^k})^p + 1$ will be divisible by $(2^{2^k} + 1)$, because $p$ is odd.

This contradicts that $(2^n + 1)$ is a prime.

Consequently, $p = 1$ and, $n = 2^k$.

## The number of positive divisors of a positive integer :~

Let, $n$ be a +ve integer $> 1$.

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \cdots p_r^{\alpha_r}, \text{ where, } \alpha_i > 0$$

if, $m$ be a positive divisor of $n$, then $m$ is of the form,

$$m = p_1^{u_1} \cdot p_2^{u_2} \cdot p_3^{u_3} \cdots p_r^{u_r}$$

where, $\boxed{0 \le u_i \le \alpha_i}$.

Thus, the positive divisors of $n$ are in one-to-one correspondence with the totality of $r$-tuples $(u_1, u_2, \cdots u_r)$.

~~The number of such~~

$u_r$ can have values $0, 1, 2, \cdots, \alpha_r$

$$\underbrace{\alpha_1+1}_{u_1} \times \underbrace{\alpha_2+1}_{u_2} \times \underbrace{\alpha_3+1}_{u_3} \times \cdots \times \underbrace{\alpha_r+1}_{u_r}$$

The number of such $r$-tuples is

$$= (\alpha_1+1) \times (\alpha_2+1)(\alpha_3+1) \cdots (\alpha_r+1)$$

(*) The total number of +ve divisors of $n$ include both 1 and $n$.

---

## $\tau(n)$ :~

The number of +ve divisors of a +ve integer $n$ is denoted by $\tau(n)$

$$\tau(n) = \tau\left(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r}\right) = (\alpha_1+1)(\alpha_2+1)\cdots(\alpha_r+1)$$

eg: $\tau(48) = \tau(2^4 \cdot 3^1) = (4+1)(1+1) = 10$

**Th:** The total number of +ve divisors of a +ve number n is odd, if and only if, n is a perfect square.

**Proof:** Let, n be a perfect square,

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r}, \quad \alpha_i > 0$$

$\therefore \alpha_i$ = even, $\because$ n is perfect square.

Now, $\tau(n) = (\alpha_1+1)(\alpha_2+1)\cdots(\alpha_r+1)$

$= \text{odd} \times \text{odd} \times \cdots \times \text{odd}$

$= \text{odd}$

Conversely, if $(\alpha_1+1)(\alpha_2+1)\cdots(\alpha_r+1) = \text{odd}$,

then, $\alpha_1, \alpha_2, \cdots \alpha_r$ = even

then, n is perfect square

---

(Q) Find the number of odd divisors of 2700

$\Rightarrow 2700 = 2^2 \cdot 3^3 \cdot 5^2$

$\therefore$ Odd divisor will contain no 2 as factor.

$\therefore$ Number of odd positive divisors

$= (0+1)(3+1)(2+1)$ ← $2^0 \times 3^3 \times 5^2$

$= 12$

---

(Q) If, $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, where $p_i$ = Primes and $\alpha_i \geq 1$, Prove that number of positive square free divisors of n is $2^k$.

$\Rightarrow \because$ Square free divisor, $m = p_1^{u_1} \cdot p_2^{u_2} \cdots p_k^{u_k}$

$\therefore 0 \leq u_i \leq 1$

$\therefore$ Number of ---- $= 2 \times 2 \times 2 \times \cdots \times 2$

$= 2^k$.

(8) Find the smallest number, having 8 positive divisors

$\Rightarrow$ $8 = 2\times2\times2 = (1+1)(1+1)(1+1) \longrightarrow p_1^1 \cdot p_2^1 \cdot p_3^1$

$= 4\times2 = (3+1)(1+1) \longrightarrow p_1^3 \cdot p_2^1$

$= 8\cdot1 = (7+1) \longrightarrow p_1^7$

$\therefore$ Among all divisors, $2^3 \cdot 3^1 = 24$ is least.

---

## The sum of all positive divisors of a positive integer :

$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r}$, where, $\alpha_i > 0$

and, $p_i$ = prime, s.t. $p_i < p_{i+1}$

Now,

$$(1+p_1+p_1^2+\cdots+p_1^{\alpha_1}) \times (1+p_2+p_2^2+\cdots+p_2^{\alpha_2}) \times \cdots \times (1+p_r+p_r^2+\cdots+p_r^{\alpha_r})$$

Each term in the product $= p_1^{u_1} \cdot p_2^{u_2} \cdots p_r^{u_r}$, where, $0 \le u_i \le \alpha_i$ is a divisor of $n$,

and conversely every +ve divisors of $n$ is a term in the product

$\therefore$ Hence the sum of all positive divisors of $n$

$$= (1+p_1+\cdots+p_1^{\alpha_1}) \cdot (1+p_2+\cdots+p_2^{\alpha_2}) \cdots (1+p_r+p_r^2+\cdots+p_r^{\alpha_r})$$

$$= \frac{p_1^{\alpha_1+1}-1}{p_1-1} \times \frac{p_2^{\alpha_2+1}-1}{p_2-1} \times \cdots \times \frac{p_r^{\alpha_r+1}-1}{p_r-1}$$

---

**$\sigma(n)$ :~** The sum of all positive divisors of a positive number $n$ is denoted by $\sigma(n)$.

$\therefore \sigma(n) = \sigma(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r})$

$$= \frac{p_1^{\alpha_1+1}-1}{p_1-1} \times \frac{p_2^{\alpha_2+1}-1}{p_2-1} \times \cdots \times \frac{p_r^{\alpha_r+1}-1}{p_r-1}$$

## Number Theoretic function:

A fn., whose domain is the set of all +ve integers is said to be a number-theoretic fn. or an arithmetic fn.

- A number-theoretic fn. is called multiplicative if $f(mn) = f(m) \cdot f(n)$, for all integers $m, n$ s.t; $m, n$ are coprime.

---

**Th:** $\tau(n)$ and $\sigma(n)$ are both multiplicative fn.

~~$\tau(mn) = \tau(m) \cdot \tau(n)$~~

(i) $\tau(m.n) = \tau(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_r^{\alpha_r} \times q_1^{\beta_1} \cdot q_2^{\beta_2} \cdots q_k^{\beta_k})$

$= (\alpha_1+1)(\alpha_2+1)\cdots(\alpha_r+1) \times (\beta_1+1)(\beta_2+1)\cdots(\beta_k+1)$

$= \tau(m) \times \tau(n)$

(ii) $\sigma(mn) = \sigma(m)(\sigma_n)$

---

## Perfect number :~

A positive integer $n$ is said to be a perfect number, if, $n$ be the sum of all its positive divisors excluding itself,

i.e, $\sigma(n) = 2n$

∵ By definition, $\sigma(n) - n = n$

eg: (i) $6 = 1 \times 2 \times 3$

$= 1+2+3$

$\sigma(6) = (1+2+3)+6$

$= 6+6 = 2 \times 6$

Similarly,

$\sigma(n) = (1+\cdots\cdots)+n$

$= n+n = 2n$

(ii) $28 = 2^2 \times 7$

∴ all positive divisors =

1, 2, 4, 7, 14, 28

∴ $1+2+4+7+14 = 28$

(9) Find the sum of all even positive divisors of 2700.

$\Rightarrow 2700 = 2^2 \cdot 3^3 \cdot 5^2$

Therefore each term in the product $(1+2+2^2)(1+3+3^2+3^3)(1+5+5^2)$, is a positive divisor of 2700 and conversely.

∴ The even positive divisors of 2700 are given by the different terms of the product

$$(2+2^2)(1+3+3^2+3^3)(1+5+5^2).$$

∴ The sum of even positive divisors

$$= (2+2^2)(1+3+3^2+3^3)(1+5+5^2) = 7440$$

---

(9) Let, $k > 1$, and $(2^k - 1)$ be a prime. If, $n = 2^{k-1} \cdot (2^k - 1)$, then prove that $n$ is a perfect number.

⇒ We have to prove, $\sigma(n) = 2n$

Now, $2^k - 1$ is an odd prime, say $p$.

∴ $\sigma\left(2^{k-1} \cdot (2^k - 1)\right)$

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

$= \sigma(2^{k-1}) \cdot \sigma(p)$ [∵ $2^{k-1}$ and $p$ are coprime]

Now, $\sigma(2^{k-1}) = 1 + 2 + 2^2 + \cdots + 2^{k-1} = 2^k - 1$

and, $\sigma(p) = 1 + p$ [∵ $p$ is prime]

∴ $\sigma(n) = \sigma(2^{k-1}) \cdot \sigma(p) = (2^k - 1) \times (1+p)$

$= (2^k - 1) \times 2^k = 2 \times \{2^{k-1} \times (2^k - 1)\} = 2n$

∴ $\sigma(n) = 2n$ ∴ $n$ is perfect number.

(*) This example shows that, if $2^n - 1$ $(n > 1)$ is a prime, then the number $2^{n-1}(2^n - 1)$ is a perfect number.

---

## Mersenne Number :—

The numbers of the form, $M_n = 2^n - 1$ $(n > 1)$ are called Mersenne Number, named after Mersenne, a French monk.

## Mersenne Prime :—

The primality of $M_n$ requires $n$ must be prime. If, $M_n$ be a prime, then $M_n$ is called a Mersenne Prime, and in that case, $2^{n-1}(2^n - 1)$ is a perfect number,

[i.e, $M_n (M_{n-1} + 1)$]

---

# THEORY OF CONGRUENCE

"If a number $n$ measures the difference between two numbers $a$ and $b$, then $a$ and $b$ are said to be congruent with respect to $n$, if not, incongruent". — Gauss

**Definition:** Let $n$ be a positive integer. Two numbers $a$ and $b$ are said to congruent modulo $n$, $(a \equiv b \pmod n)$, if $n$ divides the difference $(a-b)$.

**Class of residues:-**

If, $a \equiv b \pmod m$, then $b$ is said to be a residue of $a$ modulo $m$.

By divison algorithm, $\exists q$ and $r$, st:

$a = qm + r$, with $0 \leq r \leq m-1$

$\because a - qm = r \quad \therefore a \equiv r \pmod n$, and this shows that $r$ is a residue of $a$ modulo $n$.

$r$ is said to be the least non negative residue of $a$ modulo $n$, (when $0 \leq r \leq n-1$)

The set of $n$ integers, $\{0, 1, 2, \ldots, n-1\}$ is called the least non-negative residues modulo $n$.

In general, a collection of $n$ integers $a_1, a_2, \ldots, a_n$ is said to form a complete set of residues (or a complete system of residues) modulo $n$, if every integer is congruent modulo $n$ to one and only one of the $a_k$.

To put it another way, $a_1, a_2, \ldots, a_n$ are congruent modulo $n$ to $0, 1, 2, \ldots, n-1$, taken in some order.

eg: $-12, -4, 11, 13, 22, 82, 91$ constitute a complete set of residues modulo 7.

Here, $-12 \equiv 2$, $-4 \equiv 3$, $11 \equiv 4$, $13 \equiv 6$, $22 \equiv 1$, $82 \equiv 5$, $91 \equiv 0 \pmod 7$

An observation of some importance is that any $n$ integers form a complete set of residues modulo $n$, if and only if no two of the integers are congruent modulo $n$.

(*) The whole set of integers ($\mathbb{Z}$) is divided into $n$ distinct and disjoint subsets, called the residue classes modulo $n$, denoted by $\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}$, and defined by,

$$\mathbb{Z} = \bar{0} \cup \bar{1} \cup \bar{2} \cup \ldots \cup \overline{(n-1)}$$

$\bar{0} = \{ 0, \pm m, \pm 2m, \ldots \}$

$\bar{1} = \{ 1, 1 \pm m, 1 \pm 2m, 1 \pm 3m, \ldots \}$

$\bar{2} = \{ 2, 2 \pm m, 2 \pm 2m, \ldots \}$

$\vdots$

$\overline{n-1} = \{ n-1, (n-1) \pm n, (n-1) \pm 2n, \ldots \}$

Any two integers in a residue class are congruent modulo $m$ and any two integers belonging to two different residue classes are incongruent modulo $n$.

---

Th: For arbitrary integers $a$ and $b$, $a \equiv b \pmod{n}$ if and only if, $a$ and $b$ leaves the same non-negative remainder, when divided by $n$.

# Important Theorems :~

Let, $n > 1$, and, $a, b, c, d \ldots$ are arbitary integers!

(1) $a \equiv a \pmod{n}$

(2) If, $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$

(3) If, $a \equiv b \pmod{n}$, and, $b \equiv c \pmod{n}$, then, $a \equiv c \pmod{n}$

(4) If, $a \equiv b \pmod{n}$, and, $c \equiv d \pmod{n}$,

then, $a + c \equiv b + d \pmod{n}$

and, $ac \equiv bd \pmod{n}$

but, converse may not be true.

(5) If, $a \equiv b \pmod{n}$,

then, $a + c \equiv b + c \pmod{n}$

and, $ac \equiv bc \pmod{n}$

but, converse may not be true.

(6) If, $a \equiv b \pmod{n}$, then $a^k \equiv b^k \pmod{n}$

for any positive integer $k$.

But converse may not be true.

[Divison not allowed, but, addition, subtraction multiplication is allowed!]

(7) If, $ca \equiv cb \pmod{n}$, then, $a \equiv b \pmod{\frac{n}{d}}$,

where, $d = \gcd(n, c)$

(8) If, $a \equiv b \pmod{n}$, and, $d \mid n$, $d > 0$, then,

$a \equiv b \pmod{d}$

(9) $a \equiv b \pmod{n_i}$ $\forall$ $i = 1, 2, \ldots, r$, if and only if,

$a \equiv b \pmod{n}$, where, $n = \text{lcm}(n_1, n_2, \ldots, n_r)$

(10) $f(x) = a_n x^n + a_{n-1} \cdot x^{n-1} + \cdots + a_1 x + a_0$ be polynomial with integral coeff. $a_i$.

If, $a \equiv b \pmod{m}$, then, $f(a) \equiv f(b) \pmod{m}$

## Proofs:

⑤ Let, $a \equiv b \pmod n$, and, $c \equiv d \pmod n$

$\Rightarrow a - b = q_1 n$ $\quad\quad$ $\Rightarrow c - d = q_2 n$

$\therefore$ Now, $ac - bd$

$= (b + q_1 n)(d + q_2 n) - bd$

$= bd + bq_2 n + dq_1 n + q_1 q_2 n^2 - bd$

$= n(bq_2 + dq_1 + q_1 q_2 n)$

$\Rightarrow ac \equiv bd \pmod n$

---

⑥ Say, $a^k \equiv b^k \pmod n$ and, $a \equiv b \pmod n$

Now,

or, $a^k \times a \equiv b^k \cdot b \pmod n$

or $a^{k+1} \equiv b^{k+1} \pmod n$

Proved by induction.

---

⑦ $ca \equiv cb \pmod n$

$\Rightarrow ca - cb = qn$

$\Rightarrow c(a-b) = qn$ ——— (i)

Let, $\gcd(n, c) = d$

$\therefore \exists$ coprimes $r$ and $s$, s.t.,

$n = dr$, $c = ds$

From (i), $ds(a-b) = qdr$

or $s(a-b) = qr$

$\therefore r \mid s(a-b)$ and, $\gcd(r, s) = 1$

From Euclid's lemma, $r \mid (a-b)$

$\therefore a \equiv b \pmod r \Rightarrow a \equiv b \pmod{\frac{n}{d}}$ (Proved)

**Corollary:**

(i) If, $ca \equiv cb \pmod{n}$ and, $\gcd(n, c) = 1$,
then, $a \equiv b \pmod{n}$

(ii) If, $ca \equiv cb \pmod{p}$, and, $p \nmid c$, where $p$ is a prime number, then, $a \equiv b \pmod{p}$

(iii) If, $ab \equiv 0 \pmod{n}$ and, $\gcd(a, n) = 1$, then,
$b \equiv 0 \pmod{n}$.

(iv) When, $ab \equiv 0 \pmod{p}$, with $p$ being a prime, then either $a \equiv 0 \pmod{p}$, or, $b \equiv 0 \pmod{p}$.

**Problems //:**

(1) Show that, $41 \mid 2^{20} - 1$

$41 \overline{)32}\,(1$
$\underline{41}$
$-9$

$\Rightarrow 2^5 = 32 \pmod{}$ $\therefore 2^5 \equiv 32 \pmod{41}$
$\equiv -9 \pmod{41}$

$41 \overline{)81}\,(2$
$\underline{82}$
$-1$

or, $(2^5)^4 \equiv (-9)^4 \pmod{41}$

or, $2^{20} \equiv (81)^2 \equiv (-1)^2 \pmod{41}$

or, $2^{10} \equiv 1 \pmod{41}$

or $2^{10} - 1 \equiv 0 \pmod{41}$

(2) Find the remainder obtained upon dividing the sum, $1! + 2! + 3! + \cdots + 100!$, by 12.

$\Rightarrow 4! \equiv 24 \equiv 0 \pmod{12}$

$\Rightarrow (4+i)! \equiv 0$

$\therefore 1! + 2! + 3! + 4! + \cdots + 100!$
$\equiv 1! + 2! + 3! + 0 + 0 + \cdots + 0 \equiv 1 + 2 + 6 \equiv 9 \pmod{12}$

(3) If, $a \equiv b \pmod{n}$, show that,
$\gcd(a, n) = \gcd(b, n)$

$\Rightarrow a \equiv b \pmod{n}$

$\Rightarrow a - b = qn$

Let, $\gcd(a, n) = d_1$

$\therefore$

---

(4) Find the remainders when $2^{50}$ and, $41^{65}$ are divided by 7.

$\Rightarrow$ (a) $2^3 \equiv 8 \equiv -1 \pmod{7}$

$\therefore 2^{50} \equiv (2^3)^{16} \cdot 2^2$

$\equiv (-1)^{16} \times 2^2 \equiv 4 \pmod{7}$

(b) $41 \equiv -1 \pmod{7}$

$7 \overline{)41}(6$
$-1$

or, $(41)^{65} \equiv (-1)^{65}$

$\equiv -1$

$7 \overline{)-1}(6$
$-7$
$6$

$\equiv 6 \pmod{7}$

(5) What is the remainder, when the following sum is divided by 4 ?

$$1^5 + 2^5 + 3^5 + \cdots + 99^5 + 100^5$$

$$\Rightarrow 1^5 + 2^5 + 3^5 + \cdots + 99^5 + 100^5$$

$$\equiv 1^5 + 3^5 + \cdots + 99^5 \quad \left[\because \text{All } (\text{even})^5 \equiv 0 \pmod 4\right]$$

$$\equiv \left(1^5 + 5^5 + 9^5 + \cdots + 97^5\right) + \left(3^5 + 7^5 + 11^5 + \cdots + 99^5\right)$$

→ Numbers of $(4n+1)$-form

→ Numbers of $(4n-1)$-form

$$\equiv (1 + 1 + 1 + \cdots + 1) + (-1 - 1 - 1 - \cdots - 1)$$

$\because 1 \equiv 1$ and, $3 \equiv -1$

$\therefore 5 \equiv 1$ $\quad 7 \equiv -1$

$\therefore 9 \equiv 1$ $\quad 11 \equiv -1$

$\pmod 4$

$$\equiv 25 - 25$$

$$\equiv 0 \pmod 4$$

---

(6) Prove that, the integer, $53^{103} + 103^{53}$ is divisible by 39.

$$\Rightarrow 53 \equiv 14 \pmod{39}$$

$$39 \overline{)\,53\,(\,1} \quad 39 \quad 14$$

and, $103 \equiv -14 \pmod{39}$

(7) Prove that $111^{333} + 333^{111}$ is divisible by 7.

$\Rightarrow 111 \equiv -1 \pmod 7$

$\therefore (111)^{333} \equiv (-1)^{333} \equiv -1$

$\therefore 333 \equiv 4$

$\therefore (333)^{111} \equiv (4)^{111}$

$4^3 \equiv 1 \pmod 7$

$\equiv (4^3)^{37} \equiv (1)^{37} \equiv 1$

$\therefore (111)^{333} + (333)^{111} \equiv -1 + 1 = 0 \pmod 7$

7 | 111 (16
7
41
42
-1

7 | 333 (47
28
53
49
4

---

(6) Prove that $53^{103} + 103^{53}$ is divisible by 39.

$\Rightarrow$ Now, $39 = 3 \times 13$

$\therefore 53 \equiv 1 \pmod{13}$

or, $53^{103} \equiv 1 \pmod{13}$ — (i)

and, $103 \equiv -1 \pmod{13}$

or, $103^{53} \equiv -1 \pmod{13}$ — (ii)

(i) + (ii) $\Rightarrow$

$53^{103} + 103^{53} \equiv 1 - 1 \equiv 0 \pmod{13}$

$\therefore 13 \mid (53^{103} + 103^{53})$ — (iii)

13 ) 53 ( 4
52
1

Alternative,

$53 \equiv 14$

Now, $(53)^2 \equiv (14)^2 \equiv 196 \equiv 1$

$\therefore (53)^{103} \equiv 53 \equiv 14$

and,

$103 \equiv 14$

$\therefore (103)^2 \equiv (-14)^2 \equiv 196 \equiv 1$

$\therefore (103)^{53} \equiv 103 \equiv -14$

$\therefore 53^{103} + 103^{53} \equiv 0$

Again, $53 \equiv -1 \pmod 3$

and, $103 \equiv 1 \pmod 3$

$\therefore 53^{103} + 103^{53} \equiv (-1)^{103} + (1)^{53} \equiv -1 + 1 \equiv 0 \pmod 3$

$\therefore 3 \mid (53^{103} + 103^{53})$ ——— (iv)

From (iii) and (iv),

$13 \mid (53^{103} + 103^{53})$ and $3 \mid (53^{103} + 105^{53})$ and 3 and 13 are coprime

$\therefore 3 \times 13 \mid (53)^{103} + (103)^{53}$

or, $39 \mid (53)^{103} + (103)^{53}$ (Proved)

---

(8) Prove that, $7 \mid (5^{2n} + 3.2^{5n-2})$

$\Rightarrow 5^{2n} + 3.2^{5n-2}$

$\equiv 25^n + 3.2^{5n-2} \pmod 7$

$\equiv 4^n + 3.2^{5n-2}$

$\equiv 2^{2n} + 3.2^{5n-2} \equiv 2^{2n}(1 + 3.2^{3n-2})$

$\equiv 2^{2n}(1 + (-4).2^{3n-2})$ [$\because 3 \equiv -4 \pmod 7$]

$\equiv 2^{2n}(1 - 2^{3n})$

$\equiv 2^{2n}(1 - 8^n) \equiv 2^{2n}(1 - 1^n)$ [$\because 8 \equiv 1$]

$\equiv 2^{2n}(1-1) \equiv 0$

$\therefore 7 \mid (5^{2n} + 3.2^{5n-2})$ (Proved)

---

Alternative: $5^2 \equiv 25 \equiv 4 \quad \therefore 5^{2n} \equiv 4^n$

and, $2^5 \equiv 4$, or, $2^{5n} \equiv 4^n$, or, $2^{5n}.4^{-1} \equiv 4^n.4^{-1} \pmod 7$ [$\because \gcd(4,7) = 1$]

or, $2^{5n-2} \equiv 4^{n-1}$

$\therefore 5^{2n} + 3.2^{5n-2} \equiv 4^n + 3.4^{n-1} \equiv 4.4^{n-1} + 3.4^{n-1} \equiv 4^{n-1} \times 7 \equiv 0$

(9) Prove that, $13 \mid 3^{n+2} + 4^{2n+1}$

$\Rightarrow 3^{n+2} + 4^{2n+1}$

$\equiv 9.3^n + 4.(16)^n \equiv 9.3^n + 4.3^n$ [$\because 16 \equiv 3 \pmod{13}$]

$\equiv 3^n(9+4) \equiv 3^n \times 13 \equiv 0 \pmod{13}$

---

(10) Prove that, $27 \mid 2^{5n+1} + 5^{n+2}$

$\Rightarrow 2^{5n+1} + 5^{n+2} \equiv 2.32^n + 25.5^n$

$\equiv 2 \times 5^n + (-2).5^n$ [$\because 32 \equiv 5 \pmod{27}$ and, $25 \equiv -2$]

$\equiv 0$

---

(11) Prove that, $43 \mid 6^{n+2} + 7^{2n+1}$

$\Rightarrow 6^{n+2} + 7^{2n+1}$

$\equiv 36.6^n + 7.49^n$

$\equiv (-7).6^n + 7.(6)^n$ [$\because 36 \equiv -7$, $49 \equiv 6 \pmod{43}$]

$\equiv 0$

---

(12) Prove that, if $a$ is an odd integer, then, $a^2 \equiv 1 \pmod 8$

$\Rightarrow a^2$

$\equiv (2k+1)^2 \equiv 4k^2+4k+1 \equiv 4k(k+1) + 1$

$\equiv 4 \times 2m + 1 \equiv 8m + 1 \equiv 1 \pmod 8$

Alternative: $a = \begin{cases} 4k+1 \\ \text{or } 4k \end{cases}$

---

(13) For any integer, $a$, $a^4 \equiv 0$ or, $1 \pmod 5$

$\Rightarrow$ Let, $a = 5q + r$, $0 \le r < 4$

$\therefore$ if, $a = 5q$, then $a \equiv 0$, or, $a^4 \equiv 0 \pmod 5$

if, $a = 5q+1$, then $a \equiv 1$, or, $a^4 \equiv 1 \pmod 5$

if, $a = 5q+2$, then, $a \equiv 2$, or, $a^4 \equiv 2^4 \equiv 16 \equiv 1$

if, $a = 5q+3$, then $a \equiv -2$, or, $a^4 \equiv (-2)^4 \equiv 1$

if, $a = 5q+4$, then $a \equiv -1$, or, $a^4 \equiv 1$

(14) for any integer $a$, $a^3 \equiv 0, 1,$ or $6 \pmod 7$

⇒ Let, $a = 7q + r$, $0 \le r \le 6$

if $a = 7q$, then, $a \equiv 0$, or, $a^3 \equiv 0 \pmod 7$

if $a = 7q+1$, then $a \equiv 1$, or $a^3 \equiv 1$

if $a = 7q+2$, then, $a \equiv 2$, or, $a^3 \equiv 2^3 \equiv 8 \equiv 1$

if $a = 7q+3$, then, $a \equiv 3$, or $a^3 \equiv 3^3 \equiv 27 \equiv 6$

if, $a = 7q+4$, then $a \equiv 4$, or, $a^3 = 4^3 = (2^3)^3 \equiv 1^3 \equiv 1$

if, $a = 7q+5$, then, $a \equiv -2$, or, $a^3 \equiv (-2)^3 \equiv -8 \equiv -1 \equiv 6$

if, $a = 7q+6$, then $a \equiv -1$, or $a^3 \equiv -1 \equiv 6$

Alternative :—

Any integer $a \in \mathbb{Z}$, is of the form $\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}$, or, $\bar{6} \pmod 7$

if $a \equiv \bar{0}$, $a^3 \equiv (\bar{0})^3 \equiv \bar{0}$

if $a \equiv \bar{1}$, then, $a^3 \equiv (\bar{1})^3 \equiv \bar{1}$

if, $a \equiv \bar{2}$, then, $a^3 \equiv (\bar{2})^3 \equiv (\bar{8}) \equiv \bar{1}$

---

(15) If the integer $a$ is not divisible by 2 or 3, then $a^2 \equiv 1 \pmod{24}$

⇒ Let, $a = (2\times3)q + r = 6q + r$

Now, ∵ $a$ is not divisible by 2 or, 3,

∴ $a$ is of the form, $6q+1$, $6q+5$. [∵ $6q, 6q+2, 6q+3, 6q+4$ is divisible by 2 or 3]

if $a = 6q+1$,

$a^2 \equiv 36q^2 + 12q + 1 \pmod{24}$

$\equiv 12q^2 + 12q + 1$

$\equiv 12q(q+1) + 1$

$\equiv 12 \times 2m + 1$

$\equiv 24m + 1 \equiv 1$

If, $a = 6q+5$

$a^2 \equiv 36q^2 + 60q + 25$

$\equiv 12q^2 + 12q + 1$

$\equiv 1$

(16) Prove, whenever $ab \equiv cd \pmod{n}$ and $b \equiv d \pmod{n}$ with $\gcd(b, n) = 1$, then $a \equiv c \pmod{n}$

$\Rightarrow ab \equiv cd \pmod{n}$

or, $ab \equiv c \times b \pmod{n}$ $\quad [\because b \equiv d \pmod{n}]$

~~and $\gcd(b, n) = 1$~~

$\therefore a \equiv c \pmod{\frac{n}{\gcd(b, n)}}$

or $a \equiv c \pmod{n}$

---

(18) If, $a \equiv b \pmod{n_1}$, and $a \equiv c \pmod{n_2}$, prove that $b \equiv c \pmod{n}$, where, $n = \gcd(n_1, n_2)$

$\Rightarrow a \equiv b \pmod{n_1}$ and, $a \equiv c \pmod{n_2}$

or, $a - b = n_1 q$ or $a - c = n_2 k$

Now, $\gcd(n_1, n_2) = n$

$\therefore n_1 = nr$, $n_2 = ns$, where $r$ and $s$ are coprime.

$\therefore a - b = nrq$, and, $a - c = nsk$ — (i) — (ii)

(ii) $-$ (i) $\Rightarrow$

$b - c = n(sk - rq)$

$\Rightarrow b \equiv c \pmod{n}$

---

(19) Prove that, $(-13)^{n+1} \equiv (-13)^n + (-13)^{n-1} \pmod{181}$, $n \geq 1$

$\Rightarrow$ Now, $(-13)^n \equiv (-13) \times (-13)^{n-1}$

$\equiv 168 \times (-13)^{n-1}$

$\equiv (169 - 1) \cdot (-13)^{n-1} \equiv (-13)^2 \cdot (-13)^{n-1} - (-13)^{n-1}$

$\equiv (-13)^{n+1} - (-13)^{n-1}$

or, $(-13)^{n+1} \equiv (-13)^n + (-13)^{n-1} \pmod{181}$

(Proved)

Alternative (Induction) :-

For, $n = 1$, the statement holds

Suppose, $(-13)^{k+1} \equiv (-13)^k + (-13)^{k-1}$ holds for $k$.

Now, $(-13)^{k+2} \equiv -13 \times (-13)^{k+1}$

$\equiv -13 \{(-13)^k + (-13)^{k-1}\}$

$\equiv (-13)^{k+1} + (-13)^k$

$\therefore$ It holds for $k+1$.

$\therefore$ statement is true

---

(20) If, $p$ be a prime satisfying $n < p < 2n$, show that,

$$\binom{2n}{n} \equiv 0 \pmod{p}$$

$\Rightarrow$ $^{2n}C_n = \dfrac{(2n)!}{n! \cdot n!} = \dfrac{(1.2.\cdots n.)(n+1)(n+2)\cdots(n+n)}{n! \times n!}$

or, $n! \times {}^{2n}C_n = (n+1)(n+2)\cdots(n+n)$

Now, $\because n < p < 2n$ , or, $n < p < (n+n)$

$\therefore$ $p$ must be one of the factors of $(n+1)(n+2)\cdots(n+n-1)$

$\therefore p \mid (n+1)(n+2)\cdots(n+n)$

or, $p \mid n! \cdot {}^{2n}C_n$

again, $\because$ $p$ is a prime and $p > n$

$\therefore p \nmid n!$

So from Euclid's lemma,

$p \mid n! \cdot {}^{2n}C_n$ and, $\gcd(n, p) = 1$

$\therefore p \mid {}^{2n}C_n$. (Proved)

Th: $x \equiv y \pmod{n_i}$ $\forall\ i = 1, 2, \ldots, r$, (*)

if and only if $x \equiv y \pmod{n}$, where $n = \text{lcm}(n_1, n_2, \ldots, n_r)$

$\Rightarrow$ (1) $x \equiv y \pmod{n_i}$

$\Rightarrow n_i \mid (x-y)$ $\forall\ i = 1, 2, \ldots, r$

$\Rightarrow (x-y)$ is a common multiple of $n_1, n_2, \ldots, n_r$

$\Rightarrow \text{lcm}(n_1, n_2, \ldots, n_r) \mid (x-y)$ [$\because$ lcm of two numbers, always divides their common multiples]

$\Rightarrow x \equiv y \pmod{n}$

(2) Conversely,

if, $x \equiv y \pmod{n}$

then, $n \mid (x-y)$

or, $\text{lcm}(n_1, n_2, \ldots, n_r) \mid (x-y)$ ——— (i)

and, we know, $n_i \mid \text{lcm}(n_1, n_2, \ldots, n_r)$ ——— (ii)

From (i) and (ii),

$n_i \mid (x-y)$

$\Rightarrow x \equiv y \pmod{n_i}$ (Proved)

---

(21) Prove that, if $a$ is an odd integer, then,

$\forall\ n \geq 1$, $a^{2^n} \equiv 1 \pmod{2^{n+2}}$

$\Rightarrow$ We know, if $a$ is odd, then, $a^2 \equiv 1 \pmod{2^3}$

Now, let, $P(k)$ : $a^{2^k} \equiv 1 \pmod{2^{k+2}}$ is true.

or, $a^{2^k} = 1 + q \cdot 2^{k+2}$ ——— (i)

Now, $a^{2^{k+1}} = a^{2^k \cdot 2} = (a^{2^k})^2$

$= (1 + q \cdot 2^{k+2})^2$ [From (i)]

$= 1 + q \cdot 2^{k+3} + q^2 \cdot 2^{2k+4}$

$\therefore a^{2^{k+1}} = 1 + 2^{k+3} \cdot (2 + q \cdot 2^{k+1})$

$\therefore a^{2^{k+1}} - 1 = 2^{k+3} \cdot (2 + q \cdot 2^{k+1})$

$\Rightarrow a^{2^{k+1}} - 1 \equiv 0 \pmod{2^{k+3}}$

$\Rightarrow a^{2^{k+1}} \equiv 1 \pmod{2^{(k+1)+2}}$

$\therefore P(k+1)$ is true for $P(k)$

$\therefore$ Proved by induction

---

(22) Prove that, $89 \mid 2^{44} - 1$.

$\Rightarrow 2^8 \equiv -11 \pmod{89}$

$\therefore 2^8 \cdot 2^3 \equiv -88 \pmod{89}$

$\therefore 2^{11} \equiv -1 \times (-1) \pmod{89}$

$\therefore 2^{11} \equiv 1 \pmod{89}$

$\therefore 2^{44} \equiv 1^4 \equiv 1 \pmod{89} \Rightarrow 89 \mid (2^{44} - 1)$

$44 = 2 \times 2 \times 11$
$= 11 \times 4$
$= 22 \times 2$

Try, $2^{11}, 2^{22}$

$\therefore 2^{11} \equiv 2048 \equiv 1$

$\therefore (2^{11})^4 \equiv 1^4$

$\therefore 2^{44} \equiv 1$

---

(23) Prove that, $97 \mid (2^{48} - 1)$

Alternative :

Now, $44 = 2 \times 2 \times 11 = 11 \times 4$

Now, We know, $2^{11} - 1 \mid 2^{44} - 1$, $(\because 11 \mid 44)$

Now, $2^{11} - 1 = 2047 = 23 \times 89$

89 | 2047 | 23
178
167
267
A

$\therefore 89 \mid 2^{11} - 1$

$\therefore 89 \mid 2^{44} - 1$

(23) Prove that, $97 \mid 2^{48} - 1$

$\Rightarrow$ Now, $48 = 2 \times 2 \times 2 \times 2 \times 3$

$= 24 \times 2$

$= 16 \times 3$

$= 12 \times 4$

$= 8 \times 6$

Multiples of 97

$= \{97, 194, 291, 388, 485, 582, 679, 776, \ldots\}$

We should try, $2^8, 2^{12}, 2^{16}, 2^{24}$

Now, $2^8 \equiv 256 \equiv 62 \equiv -35$

$\therefore 2^{12} \equiv 2^8 \cdot 2^4 \equiv -35 \times 16 \equiv -560$

or, $2^{12} \equiv -(-22) \equiv 22$

or, $(2^{12})^4 \equiv (22)^4$

or, $2^{48} \equiv (22^2)^2 \equiv (484)^2$

$\equiv (-1)^2 \equiv 1$

or $2^{48} - 1 \equiv 0 \pmod{97}$

$\Rightarrow 97 \mid (2^{48} - 1)$ (Proved)

35 × 16 = 210, 350, 560

582 mod 560 = 22

22 × 22 = 484

Alternate: Binary exponentiation algorithm

$2^6 \equiv -33$

$\therefore 2^{12} \equiv (-33)^2 \equiv 1089 \equiv 22$

$\therefore 2^{24} \equiv (22)^2 \equiv 484 \equiv -1$

$\therefore 2^{48} \equiv 1$

---

(24) If, $a \equiv b \pmod{n}$, prove that $\gcd(a, n) = \gcd(b, n)$

$\Rightarrow$ Let, $\gcd(a, n) = d_1$

or, $a = d_1 r, n = d_1 s$

$\therefore a \equiv b \pmod{n}$

$\Rightarrow a - b = q_1 n$

$\Rightarrow d_1 r - b = q_1 d_1 s$

$\Rightarrow d_1 (r - s) = b$

$\Rightarrow d_1 \mid b$

$\Rightarrow d_1 \mid d_2$ [$\because \gcd(b, n) = d_2$] ——— (i)

$\gcd(b, n) = d_2$

or, $b = d_2 r', n = d_2 s'$

similarly, by putting, $b = d_2 r', n = d_2 s'$

we get, $d_2 \mid d_1$ ——— (ii)

From (i) and (ii), $d_1 = d_2$

## Number system :~

Given an integer $b > 1$, any positive integer $N$ can be written uniquely in terms of powers of $b$ as

$$N = a_m b^m + a_{m-1} \cdot b^{m-1} + \cdots + a_2 b^2 + a_1 b + a_0,$$

where the coeff. $a_i$ can take on the $b$ different values, $0, 1, 2, \ldots, (b-1)$.

This number may be replaced by simpler symbol,

$$N = (a_m a_{m-1} \cdots a_2 a_1 a_0)_b$$

We call this the base $b$ place-value notation for $N$.
or, base $b$ expansion of $N$.

---

**Th:** $f(x) = a_m x^m + a_{m-1} \cdot x^{m-1} + \cdots + a_1 x + a_0$ be a polynomial fn, If, $a \equiv b \pmod n$
Then, $f(a) \equiv f(b) \pmod n$

---

## Th: Divisibility by 9 :~

Let, $N = a_m \cdot 10^m + a_{m-1} \cdot 10^{m-1} + \cdots + a_1 \cdot 10 + a_0$ be the decimal representation of positive integer $N$, $0 \le a_i \le 9$
and, Let, $S = a_0 + a_1 + a_2 + \cdots + a_m$. Then,

$9 \mid N$ if and only if, $9 \mid S$.

**Proof:** Consider, $f(x) = a_m \cdot x^m + a_{m-1} \cdot x^{m-1} + \cdots + a_1 x + a_0$

Now, $10 \equiv 1 \pmod 9$

$\Rightarrow f(10) \equiv f(1) \pmod 9$

$\Rightarrow a_m \cdot 10^m + a_{m-1} \cdot 10^{m-1} + \cdots + a_1 10 + a_0$

$\equiv a_m + a_{m-1} + \cdots + a_0 \pmod 9$

$\Rightarrow N \equiv S \pmod 9$

That follows, if $S \equiv 0$, then $N \equiv 0 \pmod 9$

(*) The remainder obtained from dividing a number 9 is same as, dividing the sum of digits of that number by 9

**Th: Divisibility by 11 :~**

$N = a_m 10^m + a_{m-1} 10^{m-1} + \cdots + a_1 10 + a_0$

and, $T = a_0 - a_1 + a_2 - a_3 + \cdots + (-1)^m a_m$ (Alternating sum of digits)

Now, $N \equiv T \pmod{11}$

or, $11 \mid N$ if and only if $11 \mid T$.

**Proof:** Now, $10 \equiv -1 \pmod{11}$

$\Rightarrow f(10) \equiv f(-1) \pmod{11}$

$\Rightarrow a_m \cdot 10^m + a_{m-1} \cdot 10^{m-1} + \cdots + a_0 \equiv a_0 - a_1 + a_2 - \cdots + (-1)^m \cdot a_m$

$\Rightarrow \boxed{N \equiv T \pmod{11}}$

---

**Eg:** (i) 35078571 is divisible by 9, because,
$(3+5+0+7+8+5+7+1)$ is divisible by 9

(ii) It is also divisible by 11, because,
$(1-7+5-8+7-0+5-3)$ is divisible by 11.

---

**Divicibility by 7, 13 :~**

$10 \equiv 3 \pmod{7}$

or, $1000 \equiv 9 \equiv -1 \pmod{7}$

$10 \equiv -3 \pmod{13}$

or, $1000 \equiv -1 \pmod{13}$

Now, if, $N = a_m (1000)^m + a_{m-1} \cdot (1000)^{m-1} + \cdots + a_1 \cdot 1000 + a_0$

and, $T = a_0 - a_1 + a_2 - \cdots + (-1)^m a^m$,

then, $N \equiv T \pmod{7}$ and $N \equiv T \pmod{13}$

**eg:** (i) $N = 23146123$ is divisible by 7
because, $N = 23 \times (1000)^2 + 146 \times (1000) + 123$
and, $(123 - 146 + 23)$ is divisible by 7.

## Binary Exponential Algorithm :~

While calculating the value of $a^k \pmod n$, when $k$ is large, there is a more efficient way of obtaining the least positive residue than multiplying $a$ by itself $k$ times.

Binary exponential algorithm relies on successive squaring with a reduction modulo $n$ after each squaring. More specifically, the exponent $k$ is written in binary form, and the values $a^{2^j} \pmod n$ are calculated for the powers of 2. These partial results are then multiplied together to get the final answer.

**Eg:** Calculate, $5^{110} \pmod{131}$ :

Now, $110 = 64 + 32 + 8 + 4 + 2 = (1101110)_2$

Thus we obtain the powers $5^{2^j} \pmod{131}$ for $0 \le j \le 6$ by repeatedly squaring while at each stage reducing each result modulo 131.

$5^2 \equiv 25$

$5^4 \equiv 625 \equiv 101$

$5^8 \equiv (101)^2 \equiv 114$

$5^{16} \equiv 27$

$5^{32} \equiv 74$

$5^{64} \equiv 105$ $\pmod{131}$

When the appropriate partial results—those corresponding to the 1's in the binary expansion of 110 — are multiplied

$$5^{110} \equiv 5^{64+32+8+4+2} \equiv 5^{64} \cdot 5^{32} \cdot 5^8 \cdot 5^4 \cdot 5^2$$

$$\equiv 105 \times 74 \times 114 \times 101 \times 25 \equiv 60 \pmod{131}$$

## Problems 4.3 :—

(2)(d) The unit digits of triangular number is 0, 1, 3, 5, 6 or, 8.

⇒ A triangular number is of the form $\frac{k(k+1)}{2}$

By division alg.; $k = 10q + r$, $[0 \le r \le 9]$

$\therefore k \equiv r \pmod{10}$

$\therefore \frac{k(k+1)}{2} \equiv \frac{r(r+1)}{2} \pmod{10}$

| r | $\frac{r(r+1)}{2}$ | mod 10 |
|---|---|---|
| 0 | 0 | 0 |
| 1 | 1 | 1 |
| 2 | 3 | 3 |
| 3 | 6 | 6 |
| 4 | 10 | 0 |
| 5 | 15 | 5 |
| 6 | 21 | 1 |
| 7 | 28 | 8 |
| 8 | 36 | 6 |
| 9 | 45 | 5 |

$\therefore \frac{k(k+1)}{2} \equiv 0, 1, 3, 5, 6, \text{or}, 8$

---

(3) Find the last two digits of the number $9^{9^9}$.

⇒ We need to find $9^{9^9} \pmod{100}$

Now, $9 \equiv (-1) \pmod{10}$

or, $9^9 \equiv 9 \pmod{10} \Rightarrow 9^9 = 10k + 9$ for some $k$

Now, $9^{9^9} \equiv 9^{10k+9} \pmod{100}$

$\equiv 9^9 \cdot 9^{10k} \pmod{100}$

Now, $9^2 \equiv 81 \pmod{100}$

$9^4 \equiv 61 \pmod{100}$

$\therefore 9^9 \equiv 9^1 \cdot 9^4 \cdot 9^4 \pmod{100}$

$\equiv 61 \times 61 \times 9 \pmod{100}$

$\equiv 21 \times 9 \pmod{100}$

or, $\boxed{9^9 \equiv 89 \pmod{100}}$

$\therefore 9^{10} \equiv 89 \times 9 \equiv 01 \pmod{100}$

or, $\boxed{9^{10k} \equiv 1^k \equiv 1 \pmod{100}}$

$\therefore 9^{9^9} \equiv 9^9 \times 9^{10k} \equiv 89 \times 1 \pmod{100} \equiv 89 \pmod{100}$

---

(5) (a) Obtain the following generalization of Theorem ;

If the integer $N$ is represented in the base $b$ by

$N = a_m b^m + a_{m-1} \cdot b^{m-1} + \cdots + a_1 b + a_0$, $\boxed{0 \le a_k \le b-1}$

then, $(b-1) \mid N$ , if and only if $(b-1) \mid (a_0 + a_1 + \cdots + a_m)$

⇒ Let, $f(x) = a_m x^m + a_{m-1} \cdot x^{m-1} + \cdots + a_1 x + a_0$

Now, we are to find, $N \pmod{b-1}$

i.e, $f(b) \pmod{b-1}$

Now, $b \equiv 1 \pmod{b-1}$

$\Rightarrow f(b) \equiv f(1) \pmod{b-1}$

$\Rightarrow N \equiv a_0 + a_1 + \cdots + a_{m-1} + a_m \pmod{b-1}$

(b) Give the criteria for the divisibility of N by 3 and 8, that depend on the digits of N when written in base 9.

$f(x) = a_m \cdot x^m + a_{m-1} \cdot x^{m-1} + \cdots + a_0$

$\Rightarrow N = a_m \cdot 9^m + a_{m-1} \cdot 9^{m-1} + \cdots + a_1 \cdot 9 + a_0$ [in Base 9]

**For 3 :–**

Now, we have to obtain, $N \pmod 3$

i.e, $f(9) \pmod 3$

Now, $9 \equiv 0 \pmod 3$

$\therefore f(9) \equiv f(0) \pmod 3$

$\Rightarrow a_m \cdot 9^m + a_{m-1} \cdot 9^{m-1} + \cdots + a_0 \equiv a_0 \pmod 3$

$\Rightarrow N \equiv a_0 \pmod 3$

$\therefore$ 3 | N if and only if, 3 | $a_0$

**For 8 :–**

Now we have to obtain $N \pmod 8$

i.e, $f(9) \pmod 8$

Now, $9 \equiv 1 \pmod 8$

$\Rightarrow f(9) \equiv f(1) \pmod 8$

$\Rightarrow N \equiv a_0 + a_1 + \cdots + a_m \pmod 8$

$\therefore$ 8 | N, if and only if, 8 | $a_0 + a_1 + \cdots + a_m$

---

(c) Is the integer $(447836)_9$ divisible by 3 and 8?

$\Rightarrow a_0 = 6$

is divisible by 3

$\therefore$ So, $N = (447836)_9$ is divisible by 3.

$a_0 + a_1 + a_2 + \cdots + a_m$

$= 6 + 3 + 8 + 7 + 4 + 4$

$= 32 \longrightarrow$ is divisible by 8.

$\therefore$ So, N is divisible by 8.

(6) Working modulo 9 or 11, find the missing digits in the calculation below:

(a) $51840 \times 273581 = 1418243x040$

(b) $2x99561 = [3(523+x)]^2$

(c) $2784x = x \times 5569$

(d) $512 \times 1x53125 = 1000000000$

(a) $51840 \times 273581 \pmod 9$

$\equiv (5+1+8+4+0) \times (2+7+3+5+8+1) \pmod 9$

$\equiv 18 \times 26 \pmod 9$

$\equiv 0 \times 26 \pmod 9$

$\equiv 0$

Now, $1418243x040 \pmod 9$

$\equiv (1+4+1+8+2+4+3+x+0+4+0) \pmod 9$

$\equiv 27+x \pmod 9$

$\equiv 0+x \pmod 9$

$\equiv x \pmod 9$

$\therefore x \equiv 0 \pmod 9$

$\Rightarrow x = 9k+0 \Rightarrow x = 0$ or, $9$ ——— (i)

again, for (mod 11)

LHS $\equiv (0-4+8-1+5) \times (1-8+5-3+7-2) \pmod{11}$

$\equiv 8 \times 0 \pmod{11} \equiv 0 \pmod{11}$

RHS $\equiv 0-4+0-x+3-4+2-8+1-4+1 \pmod{11}$

$\equiv -13-x \pmod{11}$

$\therefore -x-13 \equiv 0 \pmod{11}$

$\Rightarrow x \equiv -13 \pmod{11}$

$\Rightarrow x \equiv -1 \times 2 \equiv 9 \pmod{11}$

$\Rightarrow x = 11k+9$

$\Rightarrow x = 9$ ——— (ii)

$\therefore$ from (i) and (ii), $x = 9$ (Ans)

(b) $2x99561 = \{3(523+x)\}^2$

$RHS = [3(523+x)]^2 = 9 \times (523+x)^2$

$\equiv 0 \pmod 9$

$\therefore LHS \equiv 0 \pmod 9$

or, $2+x+9+9+5+6+1 \equiv 0 \pmod 9$

or, $x + 32 \equiv 0 \pmod 9$

or, $x \equiv -32 \equiv -1 \times (-4)$ or $\equiv 4 \pmod 9$

$\Rightarrow x = 9k+4$

$\therefore x \in \{4, 13, 22, \cdots\}$

$\because 0 \le x \le 9 \Rightarrow x = 4$ (Ans)

---

(c) $2784x \equiv x \times 5569 \pmod 9$

or, $2+7+8+4+x \equiv x \times (5+5+6+9) \pmod 9$

or, $21 + x \equiv x \times 25 \pmod 9$

or, $3 + x \equiv x \times 7$

or, $6x \equiv 3 \equiv 9+3 \equiv 12 \pmod 9$

or, $6x \equiv 6 \times 2 \pmod 9$

or, $x \equiv 2 \pmod{\frac{9}{\gcd(9,6)}}$

or $x \equiv 2 \pmod 3$

$\Rightarrow x = 3k+2 \quad \therefore x = 2$, or, 5, or 8 ——— (i)

Again, $2784x \equiv x \times 5569 \pmod{11}$

or, $x - 4 + 8 - 7 + 2 \equiv x \times (9 - 6 + 5 - 5) \pmod{11}$

or, $x - 1 \equiv x \times 3 \pmod{11}$

or, $2x \equiv -1 \equiv 10 \pmod{11}$

or, $2x \equiv 2 \cdot 5 \pmod{11}$

or, $x \equiv 5 \pmod{\frac{11}{\gcd(2,11)}}$

or, $x \equiv 5 \pmod{11} \Rightarrow x = 5, 16, 27, \cdots$ ——— (ii)

From (i) and (ii), $x = 5$ (Ans)

(d) $512 \times 1 \times 53125 \equiv 1000,000,000 \pmod{11}$

or, $(2-1+5) \times (5-2+1-3+5-x+1) \equiv 0-0+0-\cdots-1 \pmod{11}$

or, $6 \times (7-x) \equiv -1 \pmod{11}$

or, $42 - 6x \equiv -1 \pmod{11}$

or, $6x \equiv 43 \equiv 10 \pmod{11}$

or, $2 \cdot 3x \equiv 2 \cdot 5 \pmod{11}$

or, $3x \equiv 5 \pmod{11}$ $\left[\because \gcd(2,11) = 1\right]$

$\therefore 3x = 11K + 5$.

$= 5, 16, 27, 38, 49, 60, \ldots\ldots$

$\therefore x = 9, 20, \ldots\ldots$ $[\because x \text{ is integer}]$

$\Rightarrow x = 9$ (Ans)

In these types of problem start by considering (mod 11) first.

---

(7) (c) An integer is divisible by 4, if and only if, the number formed by its tens and units digits is divisible by 4.

$\Rightarrow$ Let, $f(x) = a_m x^m + a_{m-1} x^{m-1} + \cdots + a_0$

Let, a number, in decimal,

$f(10) = N = a_m \cdot 10^m + a_{m-1} \cdot 10^{m-1} + \cdots + a_1 \cdot 10 + a_0$

Now, $100 \equiv 0 \pmod 4$

and, $1000 \equiv 0 \times 10 \equiv 0 \pmod 4$

$\vdots$

$(10)^k \equiv 0 \pmod 4 \quad \forall\ k \geq 2$

$\therefore f(10) \equiv a_m \times 10^m + a_{m-1} \cdot 10^{m-1} + \cdots + a_2 \cdot 100 + a_1 \cdot 10 + a_0$

$\equiv 0 + 0 + \cdots + 0 + a_1 \cdot 10 + a_0 \pmod 4$

or, $N \equiv a_1 \times 10 + a_0 \pmod 4$

$\therefore 4 \mid N$, if and only if $4 \mid (a_1 \times 10 + a_0)$.

(9) Find the remainder, when $4444^{4444}$ is divided by 9.

→ Now, $4444 \equiv 4+4+4+4 \pmod 9$

$\equiv 16$

$\equiv 7$

$\equiv -2 \pmod 9$

$\therefore (4444)^3 \equiv (-2)^3 \equiv -8 \equiv -1 \times -1 \equiv 1$

$\therefore (4444)^{4444} \equiv (4444)^{3 \times 1481} \times (4444)$

$\equiv 1^{1481} \times 4444$

$\equiv 1 \times (-2)$

$\equiv 7 \pmod 9$

---

(10) Prove that, no integer whose digits add up to 15, can be a square or cube.

→ Let, the number be, $N = a_m \cdot 10^m + a_{m-1} \cdot 10^{m-1} + \cdots + a_0$

$\therefore N \equiv a_0 + a_1 + a_2 + \cdots + a_m \equiv 15 \pmod 9$

or, $N \equiv 15 \pmod 9$

or, $N \equiv 6 \pmod 9$

Now, any number, $a = 9q + r$, $0 \le r \le 8$

$\therefore a \equiv 0, 1, 2, 3, 4, 5, 6, 7$ or, $8 \pmod 9$

$\therefore a^2 \equiv 0, 1, 4, 0, 7, 7, 0, 7,$ or, $1 \pmod 9$

or, $a^2 \equiv 0, 1, 4, 7 \pmod 9$

and, $a^3 \equiv 0, 1, 8 \pmod 9$

$\therefore$ No square or cube is congruent to 6 $\pmod 9$.

$\therefore$ Statement is true.

(11) Assuming that, $495 \mid 273x49y5$, obtain the digits $x$ and $y$.

$\Rightarrow 273x49y5 \equiv 0 \pmod{495}$

$\Rightarrow 273x49y5 \equiv 0 \pmod{9}$ $[\because 9 \mid 495]$

$\Rightarrow 2+7+3+x+4+9+y+5 \equiv 0 \pmod{9}$

$\Rightarrow 30 + x + y \equiv 0 \pmod{9}$

$\Rightarrow x+y \equiv -30 \equiv -3 \equiv 6 \pmod{9}$

$\Rightarrow x+y = 9k+6 = 6, 15, 24, \ldots\ldots$

$\because 0 \le x \le 9$ and, $0 \le y \le 9$ $\therefore 0 \le x+y \le 18$

$\therefore x+y = 6$ or, $15$ ——— (i)

Again, $273x49y5 \equiv 0 \pmod{495}$

$\Rightarrow 273x49y5 \equiv 0 \pmod{11}$ $[\because 11 \mid 495]$

$\Rightarrow 5-y+9-4+x-3+7-2 \equiv 0 \pmod{11}$

$\Rightarrow x-y+12 \equiv 0 \pmod{11}$

$\Rightarrow x-y \equiv -12 \equiv -1 \equiv 10 \pmod{11}$

$\Rightarrow x-y = 11k+10$

$\Rightarrow x-y = \ldots\ldots, -12, -1, 10, 21, \ldots$

$\Rightarrow x-y = -1$ $[\because -9 \le x-y \le 9]$

$0 \le x \le 9$

$0 \le y \le 9 \Rightarrow -9 \le -y \le 0$

$\therefore -9 \le x-y \le 9$

——— (ii)

From (i) and (ii),

if, $x+y=6 \Rightarrow 2x = 5$ i.e., $x = 2.5$ (impossible)

else if, $x+y = 15 \Rightarrow 2x = 14$, or, $x = 7$

$\therefore x = 7, y = 8$ (Ans)

(12) Determine the last 3 digits of $7^{999}$

$\Rightarrow$

$7^n \rightarrow 7, 49, 343, 2401, 16807, \ldots$

$\therefore 7^4 \equiv 2401 \pmod{1000}$

$\equiv 401 \pmod{1000}$

$\equiv (1+400) \pmod{1000}$ | 4

or, $7^{4n} \equiv (1+400)^n$

$\equiv 1^n + {}^nC_1 \cdot 400 + {}^nC_2 \cdot (400)^2 + \cdots + (400)^n$

$\equiv 1 + n \cdot 400 + 1000\left[{}^nC_2 \times 160 + \cdots + 4^n \times 10^{2n-3}\right]$

$\therefore 7^{4n} \equiv 1 + 400n \pmod{1000}$

Now, $999 = 4 \times 249 + 3$

$7)\overline{999}(249$
$8$
$19$
$16$
$39$
$36$
$3$

$\therefore 7^{999} \equiv 7^{4\times 249} \times 7^3$

$\equiv (1 + 400 \times 249) \times 343 \pmod{1000}$

$\equiv (1 + 99600) \times 343 \pmod{1000}$

$\equiv (1 + 600) \times 343 \pmod{1000}$

$\equiv 601 \times 343 \pmod{1000}$

$601 \times 343$

$1803$
$2404\times$
$1803\times$
$\cdots 143$

$\therefore 7^{999} \equiv 143 \pmod{1000}$

(13) If, $t_n$ denotes the nth triangular number, show that, $t_{n+k} \equiv t_n \pmod{k}$. Hence, $t_n$ and $t_{n+10}$ must have the same last digit.

$$\Rightarrow t_n = \frac{n(n+1)}{2}$$

$$\therefore t_{n+k} \equiv \frac{(n+k)(n+k+1)}{2}$$

$$\equiv \frac{n(n+1)}{2} \pmod{k}$$

or, $t_{n+k} \equiv t_n \pmod{k}$ (Proved)

---

(15) Find values of $n \geq 1$ for which, $1! + 2! + 3! + \cdots + n!$ is a perfect square.

⇒ Now, if a be any number,

then, $a \equiv 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 \pmod{10}$

$\therefore a^2 \equiv 0, 1, 4, 5, 6, \text{or}, 9$

Now, $1! + 2! + 3! + 4! + 5! + \cdots + n!$

$\equiv 1 + 2 + 6 + 24 + 120 + \cdots + n! \pmod{10}$

$\equiv 1 + 2 + 6 + 24 + 0 + 0 + \cdots + 0 \pmod{10}$ $\quad [\because n! \equiv 0 \pmod{10} \ \forall\ n \geq 4]$

$\equiv 3 \pmod{10}$

But a perfect square can't have 3 as last digit

Now for, $n \leq 4$,

$\sum_1^4 n! = 1! + 2! + 3! + 4! = 33 \longrightarrow$ Not perfect square

$\sum_1^3 n! = 1! + 2! + 3! = 9 \longrightarrow$ Perfect square

$\sum_1^3 n! = 1! + 2! = 3 \longrightarrow$ Not " "

$\sum_1^1 n! = 1! = 1 \longrightarrow$ Perfect square.

$\therefore$ for, $n = 1$ and $3$, $(1! + 2! + \cdots + n!)$ is perfect square.

(*) (*) (*)

(16) Show that $2^n$ divides an integer N, if and only if, $2^n$ divides the number made up of the last $n$ digits of N.

Now, $10^k \equiv 2^k \cdot 5^k \equiv 0 \pmod{2^n} \quad \forall\ k \geq n$

$\therefore N = a_m \cdot 10^m + a_{m-1} \cdot 10^m + \cdots + a_{n+1} \cdot 10^{n+1} + a_n \cdot 10^n + a_{n-1} \cdot 10^{n-1} + a_{n-2} \cdot 10^{n-2} + \cdots + a_1 \cdot 10 + a_0$

$\therefore N \equiv 0 + 0 + 0 + \cdots + a_{n-1} \cdot 10^{n-1} + a_{n-2} \cdot 10^{n-2} + \cdots + a_0 \pmod{2^n}$

or, $N \equiv a_{n-1} \cdot 10^{n-1} + a_{n-2} \cdot 10^{n-2} + \cdots + a_1 \cdot 10 + a_0 \pmod{2^n}$

or, $N \equiv \overline{a_{n-1} \cdot a_{n-2}\ a_{n-3} \cdots a_1 \cdot a_0} \pmod{2^n}$

$\therefore 2^n \mid N$ if and only if, $2^n \mid \overline{a_{n-1} \cdot a_{n-2} \cdots a_1 \cdot a_0}$

---

Eg: (i) $2 \mid N$, if and only if, $2 \mid$ last digit

(ii) $4 \mid N$, if and only if, $4 \mid$ last two digits

(iii) $8 \mid N \iff 8 \mid$ last three digit

(iv) $16 \mid N \iff 16 \mid$ last four digit

---

(17) (b) Prove that, $6 \mid N \iff 6 \mid a_0 + 4a_1 + 4a_2 + \cdots + 4a_m$

Let, $N = a_m \cdot 10^m + a_{m-1} \cdot 10^{m-1} + \cdots + a_1 10 + a_0$

Now, $10 \equiv 4 \pmod 6$

$100 \equiv 10 \times 10 \equiv 4 \times 4 \equiv 16 \equiv 4 \pmod 6$

$\therefore 10^k \equiv 4 \pmod 6 \quad \forall\ k \geq 1$

$\therefore N \equiv a_m \cdot 10^m + a_{m-1} \cdot 10^{m-1} + a_1 \cdot 10 + a_0$

or, $N \equiv 4a_m + 4a_{m-1} + \cdots + 4a_1 + a_0 \pmod 6$

(Proved)

(17) Let,

$N = a_m \cdot 10^m + a_{m-1} \cdot 10^{m-1} + \cdots + a_1 \cdot 10 + a_0$

be a decimal expansion of positive integer $N$.

(a) Proove that, 7, 11 and 13 divides $N$, if and only if, 7, 11, 13 divides the integer,

$M = (a_0 + 10a_1 + 100a_2) - (a_3 + 10a_4 + 100a_5) + (a_6 + 10a_7 + 100a_8) - (\cdots) + \cdots\cdots$

⇒ We have to proove, 7, 11, and 13 divides $N$

i.e, $\text{lcm}(7, 11, 13) \mid N$

i.e, $7 \times 11 \times 13 \mid N$

i.e, $1001 \mid N$

Now, $10^3 \equiv 1000 \equiv -1 \pmod{1001}$

or, $10^{3n} \equiv (-1)^n \equiv \begin{cases} 1 & , \text{if } n \text{ is even} \\ -1 & , \text{if } n \text{ is odd} \end{cases}$

Now, $N \equiv a_m 10^m + a_{m-1} \cdot 10^{m-1} + \cdots + a_n 10^n + a_{n-1} \cdot 10^{n-1} + a_{n-2} \cdot 10^{n-2}$

$+ \cdots + a_8 \cdot 10^8 + a_7 \cdot 10^7 + a_6 10^6 + a_5 \cdot 10^5 + a_4 10^4 + a_3 10^3$

$+ a_2 10^2 + a_1 10 + a_0$

or, $N \equiv (a_0 + a_1 \cdot 10 + a_2 \cdot 100) + 10^3 (a_3 + a_4 \cdot 10 + a_5 \cdot 100)$

$+ 10^{3\times 2} (a_6 + a_7 \times 10 + a_8 100) + 10^{3\times 3} (a_9 + a_{10} \cdot 10 + a_{11} \cdot 100)$

$+ \cdots\cdots \pmod{1001}$

$\equiv (a_0 + 10a_1 + 100a_2) - (a_3 + 10a_4 + 100a_5) + (a_6 + 10a_7 + 100a_8)$

$- \cdots\cdots \pmod{1001}$

(Prooved)

Similarly, the converse can be also prooven!

(18) Without performing divison, determine, whether 10109088 99 is divisible by 7, 11, and 13. (i.e 1001)

$\Rightarrow$ 10 10 90 88 99

$\equiv 899 - 908 + 010 - 1 \pmod{1001}$

$\equiv 0 \pmod{1001}$

$\therefore$ 10 10 90 88 99 is divisible by 1001.

---

(*) (*) (*) Generalization :

Let, $N = a_m a_{m-1} a_{m-2} \cdots a_{(n+k)} a_{(n+k-1)} \cdots a_n$

## Generalization :~

$N \pmod{10^n+1}$ and, $N \pmod{10^n-1}$

Let, $N = a_m \cdot 10^m + a_{m-1} \cdot 10^{m-1} + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$

$= \overline{a_m a_{m-1} \cdots a_{3n-1} a_{3n-2} \cdots a_{2n} a_{2n-1} a_{2n-2} \cdots a_{n+1} a_n a_{n-1} a_{n-2} \cdots a_2 a_1 a_0}$

(1) $N \equiv \overline{a_{n-1} a_{n-2} \cdots a_2 a_1 a_0} + \overline{a_{2n-1} a_{2n-2} \cdots a_{n+1} a_n} + \overline{a_{3n-1} a_{3n-2} \cdots a_{2n+1} a_{2n}} + \overline{a_{4n-1} \cdots a_{3n+1} a_{3n}} + \cdots \pmod{10^n-1}$

$\equiv$ Sum of numbers, made up with $n$ digits starting from units digits place $\pmod{10^n-1}$

(2) $N \equiv \overline{a_{n-1} a_{n-2} \cdots a_1 a_0} - \overline{a_{2n-1} a_{2n-2} \cdots a_{n+1} a_n} + \overline{a_{3n-1} \cdots a_{2n+1} a_{2n}} - \overline{a_{4n-1} \cdots a_{3n+1} a_{3n}} + \cdots \pmod{10^n+1}$

$\equiv$ Alternating Sum of numbers, made up with $n$ digits starting from unit digits place $\pmod{10^n+1}$

**Proof :~**

(1) $10^n - 1 \equiv 0 \pmod{10^n-1}$

or) $10^n \equiv 1 \pmod{10^n-1}$

Now, $N \equiv a_m \cdot 10^m + \cdots + (a_{3n-1} \cdot 10^{2n-1} + a_{2n-2} \cdot 10^{2n-2} + \cdots + a_n \cdot 10^n) + (a_{n-1} \cdot 10^{n-1} + a_{n-2} 10^{n-2} + \cdots + a_1 10 + a_0)$

$\equiv (a_0 + a_1 10 + \cdots + a_{n-1} \cdot 10^{n-1}) + 10^n (a_n + \cdots + a_{2n-2} \cdot 10^{n-2} + a_{2n-1} \cdot 10^{n-1}) + 10^{2n} (a_{2n} + a_{2n+1} \cdot 10 + \cdots + a_{3n-1} \cdot 10^{n-1}) + \cdots \pmod{10^n-1}$

$\equiv (a_0 + a_1 \cdot 10 + \cdots + a_{n-1} \cdot 10^{n-1}) + (a_n + \cdots + a_{2n-2} \cdot 10^{n-2} + a_{2n-1} \cdot 10^{n-1}) + (a_{2n} + a_{2n+1} \cdot 10 + \cdots + a_{3n-1} \cdot 10^{n-1}) + \cdots \pmod{10^n-1}$

$$N \equiv \overline{a_{n-1}a_{n-2}\cdots a_1 a_0} + \overline{a_{2n-1}a_{2n-2}\cdots a_n} + \overline{a_{3n-1}a_{3n-2}\cdots a_{2n}} + \cdots \pmod{10^n - 1}$$

We can also prove converse.

(2) $10^n + 1 \equiv 0 \pmod{10^n + 1}$

or, $10^n \equiv -1 \pmod{10^n + 1}$

∴ We can similarly prove that,

$$N \equiv \left(\overline{a_{n-1}a_{n-2}\cdots a_0}\right) - \left(\overline{a_{2n-1}\cdots a_{n+1}a_n}\right) + \left(\overline{a_{3n-1}a_{3n-2}\cdots a_{2n}}\right) - \cdots \pmod{10^n + 1}$$

**Example :**

(1) $4567892\underline{5768} \pmod{999}$ $\quad [999 = 10^3 - 1]$

$\equiv 5768 + 7892 + 0456 \pmod{999}$

$\equiv (4995 + 773) + (7992 - 100) + 456 \pmod{999}$

$\equiv 773 - 100 + 456 \pmod{999}$

$\equiv 1129 \pmod{999}$

$\equiv 130 \pmod{999}$

1129
−999
130

999
999×2 = 1998
999×3 = 2997
999×4 = 3996
999×5 = 4995
999×6 = 5994
999×7 = 6993
999×8 = 7992

**Example :**

(1) $456789\underline{257}68 \pmod{999}$ $\quad [999 = 10^3 - 1]$

$\equiv 768 + 925 + 678 + 045 \pmod{999}$

$\equiv 1693 + 723$

$\equiv (1998 - 305) + 723 \pmod{999}$

$\equiv -305 + 723 \pmod{999}$

$\equiv 418 \pmod{999}$

999
999×2 = 1998

② $4567892\,5768 \pmod{10001}$

$10001 = 10000 + 1$
$= 10^4 + 1$

$\equiv 5768 - 7892 + 0456 \pmod{10001}$

$\equiv 6224 - 7892 \pmod{10001}$

$\equiv -1668 \pmod{10001}$

$\equiv 10001 - 1668 \pmod{10001}$

$\equiv 8333 \pmod{10001}$

5768 − 456 = 6224

7892 − 6224 = 1668

10001 − 1668 = 8333

(19) (a) Given an integer N, let M be the integer formed by reversing the order of the digits of N. Verify that (N − M) is divisible by 9.

$\Rightarrow N = \overline{a_m a_{m-1} \cdots a_2 a_1 a_0}$

$\therefore M = \overline{a_0 a_1 a_2 \cdots a_{m-1} a_m}$

Now, $N \equiv a_0 + a_1 + a_2 + \cdots + a_{m-1} + a_m \pmod 9$

and, $M \equiv a_m + a_{m-1} + \cdots + a_2 + a_1 + a_0 \pmod 9$

$\therefore N - M \equiv 0 \pmod 9$

$\Rightarrow (N-M)$ is divisible by 9.

---

(b) Prove that any palindrome with an even number of digits is divisible by 11.

Let, total number of digits be $2m$

$N = a_{2m-1} \cdot 10^{2m-1} + a_{2m-2} \cdot 10^{2m-2} + \cdots + a_2 \cdot 10^2 + a_1 \cdot 10 + a_0$

$\therefore 10 \equiv -1 \pmod{11}$

$\therefore N \equiv a_0 - a_1 + a_2 - \cdots + a_{2m-2} - a_{2m-1}$ [$\because 2m-1 = \text{odd}$, $\therefore 10^{2m-1} \equiv -1$]

or, $N \equiv (a_0 - a_{2m-1}) - (a_1 - a_{2m-2}) + (a_2 - a_{2m-3}) - \cdots\cdots$

→ There will be exact $m$ pairs
$\because$ Total number of digits $= 2m$

Now, $\because N$ is palindrome.

$\therefore a_0 = a_{2m-1}$, $a_1 = a_{2m-2}$, $a_2 = a_{2m-3}$, ....

$\therefore N \equiv 0 - 0 + 0 - 0 + \cdots\cdots \pmod{11}$

or, $N \equiv 0 \pmod{11}$ (Proved)

Example: $123456654321$ is divisible by $11$

$\Rightarrow 123456654321$

$\equiv (1-2+3-4+5-6)+(6-5+4-3+2-1) \pmod{11}$

$\equiv 0 \pmod{11}$

---

(20) Given repunit $R_n$, show that,

a) $9 \mid R_n$ if and only if, $9 \mid n$

b) $11 \mid R_n$ if and only if, $n$ is even

$\Rightarrow$ (a) $R_n = 111\ldots1$ ($n$ digits of 1's)

$\therefore R_n \equiv 1+1+1+\cdots+1 \pmod{9}$

or, $R_n \equiv n \pmod{9}$

$\therefore 9 \mid R_n$ if, $9 \mid n$

(b) $R_n = 10^{n-1} + 10^{n-2} + \cdots + 10 + 1$

$\therefore R_n \equiv (-1)^{n-1} + (-1)^{n-2} + \cdots - 1 + 1 \pmod{11}$

$\equiv (1-1)+(1-1)+(1-1)+\ldots\ldots$

Let, $T = (1-1)+(1-1)+(1-1)+\ldots\ldots$

$\therefore T$ will be $0 \iff$ can group terms, which means number of terms is even

$\therefore R_n \equiv 0 \pmod{11}$ if, and only if $n$ is even.

(21) Factor the repunit, $R_6 = 111,111$ into product of primes.

⇒ Now, $111,111$

$\equiv (111) - (111) \pmod{10^3+1}$

$\equiv 0 \pmod{1001}$

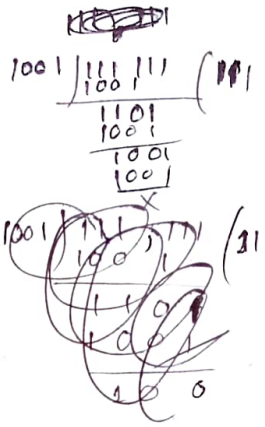
$\therefore 1001 \mid 111,111$

and, $1001 = 7 \times 11 \times 13$

$\therefore 111,111 = 7 \times 11 \times 13 \times K$

$= 7 \times 11 \times 13 \times 111$

$= 7 \times 11 \times 13 \times 3 \times 37$ (Ans)



---

(22) Explain, why the following curious calculation holds:

$1 \times 9 + 2 = 11 = R_2$

$12 \times 9 + 3 = 111 = R_3$

$123 \times 9 + 4 = 1111 = R_4$

$1234 \times 9 + 5 = 11111 = R_5$

$12345 \times 9 + 6 = 111111 = R_6$

$123456 \times 9 + 7 = 1111111 = R_7$

$1234567 \times 9 + 8 = 11111111 = R_8$

$12345678 \times 9 + 9 = 111111111 = R_9$

$123456789 \times 9 + 10 = 1111111111 = R_{10}$

⇒ We are to prove,

$(1 \times 10^{n-1} + 2 \times 10^{n-2} + 3 \times 10^{n-3} + \cdots + (n-1).10 + n) \times 9 + (n+1)$

$= R_{n+1}$

Now, $9 \times (1 \times 10^{n-1} + 2 \times 10^{n-2} + \cdots + n)$

$= (10-1)(1 \times 10^{n-1} + 2 \times 10^{n-2} + \cdots + (n-1).10 + n)$

$= 10 \times (10^{n-1} + 2 \times 10^{n-2} + \cdots + (n-1).10 + n)$

$- (1 \times 10^{n-1} + 2 \times 10^{n-2} + \cdots + n)$

$$= (10^n + 2\times10^{n-1} + 3\times10^{n-2} + \cdots + (n-1).10^2 + n.10) - (1\times10^{n-1} + 2\times10^{n-2} + \cdots + (n-1).10 + n)$$

$$= 10^n + 10^{n-1} + 10^{n-2} + \cdots + 10^2 + 10 - n$$

Now, $9\times(10^{n-1} + 2\times10^{n-2} + 3\times10^{n-3} + \cdots + n) + (n+1)$

$$= 10^n + 10^{n-1} + 10^{n-2} + \cdots + 10^2 + 10 - n + n + 1$$

$$= 1 + 10 + 10^2 + \cdots + 10^{n-1} + 10^n$$

$$= \frac{10^{n+1} - 1}{10 - 1} = \frac{10^{n+1} - 1}{9} = R_{n+1} \quad \text{(Proved)}$$

---

(23) An old and somewhat illegible invoice shows that 72 canned hams were purchased for $\$ x67{\cdot}9y$. Find the missing digits.

$\Rightarrow 72 \mid x679y$

Now, $72 = 2^3 \cdot 9$

$\therefore 2^3 \mid x679y$

$\Rightarrow x679y \equiv 79y \pmod 8$

$\therefore x679y \equiv 0 \pmod 8$

$\therefore 79y \equiv 0 \equiv 8$

$\Rightarrow 79y \equiv 0 \pmod 8$ [$\because$ divisible by 8]

$\Rightarrow 790 + y \equiv 0$, or, $6 + y \equiv 0$

$\Rightarrow y \equiv -6 \equiv 2 \pmod 8$

$\Rightarrow \boxed{y = 2}$

$8)790(98$
$\underline{72}$
$\underline{\phantom{0}70}$
$\underline{\phantom{0}64}$
$\phantom{0}6$

Now. $\because 9 \mid x6792$, $\Rightarrow x6792 \equiv 0 \pmod 9$

or, $x + 6 + 7 + 9 + 2 \equiv 0 \pmod 9$

or, $x \equiv 3$ $\therefore \boxed{x = 2,\ y = 2}$

(24) If $792 \mid \overline{13xy45z}$, find the digits $x, y, z$

$\Rightarrow$ Now, $792 = 8 \times 11 \times 9$

$8 \mid 792 \mid 99$, $72$, $72$

$\therefore \quad 8 \mid \overline{13xy45z}$

$\Rightarrow \overline{13xy45z} \equiv 0 \pmod 8$

$\Rightarrow \overline{45z} \equiv 0 \pmod 8$

$\Rightarrow 450 + 7 \equiv 0 \pmod 8$

$\Rightarrow 2 + z \equiv 0$, or, $z \equiv -2 \equiv 6 \pmod 8$

$\therefore \boxed{z = 6}$

again, $\overline{13xy45z} \equiv 0 \pmod 9$

$\Rightarrow 1+3+x+y+4+5+6 \equiv 0 \pmod 9$

$\Rightarrow x + y \equiv -18 \equiv 8 \pmod 9$

$\Rightarrow \boxed{x + y = 8}$ ——— (i)

Again, $\overline{13xy45z} \equiv 0 \pmod{11}$

$\Rightarrow z - 5 + 4 - y + x - 3 + 1 \equiv 0$

$\Rightarrow 6 - 5 + 4 - y + x - 3 + 1 \equiv 0$

$\Rightarrow x - y \equiv 8 \pmod{11}$

$\therefore \boxed{x - y = 8}$ ——— (ii)

From (i) and (ii), $\boxed{x = 8}$ $\boxed{y = 0}$

$\therefore \boxed{x = 8, y = 0, z = 6}$