$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

$$\tau(n) = (1+\alpha_1) \cdots (1+\alpha_k)$$

$$= \prod_{i=1}^{k} (1+\alpha_i).$$

The sum of all positive divisors of a positive integer.

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$$

$$\sigma(n) = \left(\frac{p_1^{\alpha_1+1}-1}{p_1-1}\right) \cdot \left(\frac{p_2^{\alpha_2+1}-1}{p_2-1}\right) \cdots \left(\frac{p_k^{\alpha_k+1}-1}{p_k-1}\right).$$

$$\begin{array}{r|l} 2 & 56 \\ \hline 2 & 28 \\ \hline 2 & 14 \\ \hline & 7 \end{array}$$

$$= \underset{p_1}{2}^{\overset{\alpha_1}{3}} \times \underset{p_2}{7}^{\overset{\alpha_2}{1}}$$

$\sigma(360)$, Prime factorization of 360

$$360 = 2^3 \cdot 3^2 \cdot 5^1$$

$$\sigma(360) = \left(\frac{2^{3+1}-1}{2-1}\right) \cdot \left(\frac{3^{2+1}-1}{3-1}\right) \cdot \left(\frac{5^{1+1}-1}{5-1}\right)$$

$$= 16 - 1 \times \cancel{26}\ 13 \times \cancel{24}\ 6$$

$$= \frac{16-1}{1} \times \frac{\cancel{26}\,3}{\cancel{2}} \times \frac{\cancel{24}\,6}{\cancel{4}}$$

$$= 15 \times 3 \times 6 = 1170.$$

2, 3, 5, 8, 9, 10, 12, 15, 18, ...

$\sigma(900) = ?$ 2821.

$7 \times 13 \times 31$

Note: $\tau(n)$, $\sigma(n)$, they both are multiplicative functions.

$\tau(m.n) = \tau(m).\tau(n)$, $\sigma(mn) = \sigma(m).\sigma(n)$.

m, n ⟶ relatively prime to each other.

$\tau(n)$ → No of positive divisors of 'n'.

$\sigma(n)$ → Sum of those positive divisors of 'n'.

$\tau(56) = 2, 1, 56, 4, \ldots$

$\sigma(n) \to 2 + 1 + 56 + 4 + \ldots$

If $d_1, d_2, \ldots d_K$ be the list of all +ve divisors of $n \in \mathbb{Z}^+$, P.T:

$$\frac{1}{d_1} + \frac{1}{d_2} + \cdots + \frac{1}{d_K} = \frac{\sigma(n)}{n}.$$

<u>Solⁿ:</u> $d_i \rightarrow$ positive divisor of n.

$d_i \mid n$, $n/d_i \rightarrow$ <u>positive divisor.</u>

$d_1)n(d_3$

$\frac{n}{x}$

$n/d_1, \; n/d_2, \; \ldots \; n/d_K$

$\downarrow \quad \downarrow \quad \downarrow$

$d_2 / d_3 / d_4 \quad - \; - \; - .$

$$\frac{n}{d_1} + \frac{n}{d_2} + \cdots + \frac{n}{d_K} = \boxed{d_2 + d_1 + d_5 + \cdots + d_K}$$

$$\Rightarrow n\left(\frac{1}{d_1} + \cdots + \frac{1}{d_K}\right) = \underbrace{d_1 + \cdots + d_K}$$

$$\Rightarrow n\left(\frac{1}{d_1} + \cdots + \frac{1}{d_K}\right) = \sigma(n).$$

$$\Rightarrow \sum_{i=1}^{K} 1/d_i = \sigma(n)/n.$$

PROVED.

Congruence

Defn: Let 'm' be a fixed positive integer. Two int. a and b are said to be <u>congruent modulo m</u> if $(a-b)$ is divisible by m.

$$a \equiv b \pmod{m}.$$
$$\hookrightarrow \quad m \mid (a-b).$$

e.g.: $m = 3$

$a = 1$, $b = 4$

$$1 \equiv 4 \pmod{3}$$

$3 \mid (1-4)$ i.e $3 \mid -3$.

$$-2 \equiv 1 \pmod{3}$$
$$3 \mid (-2-1) \Rightarrow 3 \mid -3.$$

$$6 \equiv 0 \pmod{3}$$

$$35 \equiv 2 \pmod{3}$$
$$\hookrightarrow 3 \mid 33.$$

Thm: For any two integers a and b, $a \equiv b \pmod{m}$, if and only if a and b leave the same remainder when divided by m.

Let, $m = 5$, $a = 21$, $b = -14$.

$$5 \overline{)21} \, (4$$
$$\underline{20}$$
$$\underline{1}$$

$$-14 = -3 \cdot 5 + 1.$$
$$21 = 4 \cdot 5 + 1$$

$$21 \equiv -14 \pmod{5}.$$

Properties :-

1. $a \equiv a \pmod{m}$

2. $a \equiv b \pmod{m}$, then $b \equiv a \pmod{m}$

$$m \mid a-b \rightarrow m \mid b-a \Rightarrow -(a-b)$$

3. $a \equiv b \pmod{m}$, $b \equiv c \pmod{m}$

   then, $a \equiv c \pmod{m}$.

'Congruence' relation is an equivalence Relation.

4. $a \equiv b \pmod{m}$, then for any $c \in \mathbb{Z}$

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

$$a \cdot c \equiv b \cdot c \pmod{m}.$$

5. $a \equiv b \pmod{m}$ and $c \equiv d \pmod{m}$ then.

$$a + c \equiv b + d \pmod{m}.$$

$$ac \equiv bd \pmod{m}.$$

6. $a \equiv b \pmod{m}$ and $d \mid m$, $d > 0$, then $a \equiv b \pmod{d}$.

Residue of a modulo 'm.'

If $a \equiv b \pmod{m}$ then b is said to be a

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

By division Algorithm, $q, r \in \mathbb{Z}$

$$a = qm + r. \qquad 0 \le r \le m-1.$$

$$a - r = qm. \implies m \mid a - r.$$

$a \equiv r \pmod{m}$. so 'r' is a residue.

remainder $\longrightarrow$ least non-negative residue of a modulo m.

Let, 'a' be any arbitrary integer. , $m \mid a$

remainder of a when divided by m

$$\in \{0, 1, \ldots\ m-1\}.$$

The whole set of integers is divided into m distinct and disjoint sub-sets called residue classes of modulo m.

$$\bar{0}, \bar{1}, \bar{2}, \ldots \overline{m-1}.$$

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

$\overline{0} = \{0, \pm m, \pm 2m, \dots\}$.

$\overline{1} = \{1, 1 \pm m, 1 \pm 2m, \dots\}$

$\overline{2} = \{2, 2 \pm m, 2 \pm 2m, \dots\}$.

$\vdots$

$\overline{m-1} = \{(m-1), (m-1) \pm m, (m-1) \pm 2m, \dots\}$.

$\frac{-15}{2} = -7.5$

$b =$

$a \equiv b \pmod{m}$

negative

$\overline{(-1)} = \dots,$

$a = 25, \; b = -2$

$a \equiv b \pmod 3$

$25 \equiv -2 \pmod 3$

$-2 \equiv 1 \pmod 3$

$$\begin{array}{r} 3 \,)\, 25 \,(\, 8 \\ 24 \\ \hline 1 \end{array}$$

$\underline{\text{Th}^m}$: If $a \equiv b \pmod m$, then $a^n \equiv b^n \pmod m$ for all positive integers n.

$9^2 \equiv 7^2 \pmod 8$

$\not\Rightarrow 9 \equiv 7 \pmod 8$

$$\begin{array}{r} 81 \\ 49 \\ \hline 32 \end{array}$$

Converse is not true. !

Th^m. If $ax \equiv ay \pmod m$ and a is prime

Thm: If $ax \equiv ay \pmod{m}$ and a is prime to m, then $x \equiv y \pmod{m}$.

$g.c.d(a, m) = 1$.

$a = 3.\ 2 \equiv 3.4 \pmod{6}$ $\quad$ $g.c.d(3, 6) \neq 1$.

$\not\Rightarrow 2 \equiv 4 \pmod{6}$

$6 \nmid -2$.

Thm: If $d = gcd(a, m)$, then $ax \equiv ay \pmod{m}$
$\Leftrightarrow x \equiv y \pmod{m/d}$

$g.c.d(3,6) = 3$. $\quad 2 \equiv 4 \pmod{6/3} \Rightarrow 2 \equiv 4 \pmod{2}$

\# If $ax \equiv ay \pmod{m}$ and $a \mid m$.
Then, $x \equiv y \pmod{m/a}$.

Thm: $x \equiv y \pmod{m_i}$ for $i = 1, 2, \ldots r$
$\Leftrightarrow x \equiv y \pmod{m}$, where $m = [m_1, \ldots m_r]$, the lcm $m_1, m_2, \ldots m_r$.

$x \equiv y \pmod{m_1}$

$x \equiv y \pmod{m_2}$ $\quad \ldots\ldots$

$x \equiv y \pmod{m}$

$$x \equiv y \pmod{m}$$

Thm: $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0$

$a_i \in \mathbb{Z}$

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

$\Rightarrow f(a) \equiv f(b) \pmod{m}$

i.e. $m \mid f(a) - f(b)$.

Divisibility Test

$$n = a_m 10^m + a_{m-1} 10^{m-1} + \dots + a_1 10 + a_0.$$

$$0 \le a_k \le 9, \quad k = 0, 1, \dots m.$$

$$S = a_0 + a_1 + \dots a_m.$$

$$T = a_0 - a_1 + \dots + (-1)^m a_m.$$

i) n is divisible by 2 if and only if a_0 is divided by 2

$$2 \mid a_0$$

ii) $9 \mid n$, iff S is divisible by 9.

iii) $11 \mid n$, iff T is divisible by 11.

H/W Find the least positive residues in

1. $3^{36} \pmod{77}$.

1. $3^{36} \pmod{77}$.

2. Use theory of congruence, Proof.

$$7 \mid 2^{5n+3} + 5^{2n+3} \quad \forall\, n \geq 1.$$

3. P.T $19^{20} \equiv 1 \pmod{181}$.