Congruences

$a \equiv b \pmod{n}$

$\Leftrightarrow n \mid a-b$

Ex:- $8 \equiv 3 \pmod 5$, $8 \equiv -2 \pmod 5$ $\Big\}$ $3 \equiv -2 \pmod 5$

Note:- $a \equiv b \pmod n$

$\Rightarrow a - b = nk$

$\Rightarrow a = nk + b$

$\Rightarrow$ b is the remainder when a is divided by n.

Properties:- For $n > 1$

(a) $a \equiv a \pmod n$

(b) $a \equiv b \pmod n \Rightarrow b \equiv a \pmod n$

(c) $a \equiv b \pmod n$ and $b \equiv c \pmod n$

$\Rightarrow a \equiv c \pmod n$

(d) $a \equiv b \pmod n$, $c \equiv d \pmod n$ $\Rightarrow$ $a+c \equiv b+d \pmod n$, $ac \equiv bd \pmod n$

(e) $a \equiv b \pmod n$

$$\Rightarrow \begin{cases} a+c \equiv b+c \pmod n \\ ac \equiv bc \pmod n \end{cases}$$

(f) $a \equiv b \pmod n$

$\Rightarrow a^k \equiv b^k \pmod n$ for any +ve integer k

Proof :- (c) $a \equiv b$, $b \equiv c$ $\Rightarrow a \equiv c \pmod n$

$a - b = nk$

$b - c = nh$

$a - c = (a-b) + (b-c)$

$= n(h+k) \Rightarrow a \equiv c \pmod n$

Theorem:- If $ca \equiv cb \pmod{n}$ then $a \equiv b \pmod{n/d}$ where $d = g.c.d(c, n)$.

Proof:- $n \mid ca - cb = c(a-b)$

$\Rightarrow c(a-b) = kn$, (k - integer)

$d = gcd(c, n) \Rightarrow \begin{cases} c = dq \\ n = ds \end{cases}$

$\therefore dq(a-b) = k(ds)$

$\Rightarrow q(a-b) = ks$

$\Rightarrow s \mid q(a-b)$

$g.c.d(q, s) = 1$

$\Rightarrow s \mid a-b$ (Euclid's lemma)

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

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

Corollary:- $ca \equiv cb \pmod{n}$

and $\text{g.c.d}(c, n) = 1$

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

Ex:- $24 \equiv 9 \pmod{15}$

i.e., $8 \times 3 \equiv 3 \times 3 \pmod{15}$

$\Rightarrow 8 \equiv 3 \left(\mod \frac{15}{3}\right)$

$\Rightarrow 8 \equiv 3 \pmod{5}$

Equivalence relation:-

(a) reflexivity $(a \equiv a)$

(b) Symmetry $(a \equiv b \Rightarrow b \equiv a)$

(c) transitivity $(a \equiv b,\ b \equiv c \Rightarrow a \equiv c)$

⇒ "$\equiv$" is an equivalence relation.

Equivalence Class:-

$\{\overline{0}, \overline{1}, \overline{2}, \cdots, \overline{n-1}\}$ is the Complete set of residues modulo n.

i.e., any integer will have remainder either $0, 1, 2, \cdots$ or $n-1$.

$\overline{0}$ = class containing integers which have remainder 0 when divided by n. (i.e., multiples of n)

$\overline{1}$ = Class containing integers which have remainder 1 when divided by n.

etc.

Ex:- The equivalence classes of with respect to mod 5 are $\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}$.

$\bar{0} = \{\ldots\ldots, -10, -5, 0, 5, 10, \ldots\ldots\}$

$\bar{1} = \{\ldots\ldots, -9, -4, 1, 6, 11, \ldots\ldots\}$

etc.

$Z_n = \{\bar{0}, \bar{1}, \bar{2}, \ldots\ldots, \overline{n-1}\}$ is the complete set of residues modulo n.

Ex:- $a^2 \equiv b^2 \pmod{n}$

$\not\Rightarrow a \equiv b \pmod{n}$

ex:- $5^2 \equiv 4^2 \pmod{3}$

But $5 \not\equiv 4 \pmod{3}$

Ex:- If $a \equiv b \pmod{n}$, then

$g.c.d(a, n) = g.c.d(b, n)$

Proof:- $n \mid a-b \Rightarrow a-b = kn$

Let $d = g.c.d.(a, n)$

$\Rightarrow a = dr$ and $n = ds$.

$\therefore a-b = kn \Rightarrow dr - b = kds$

$\Rightarrow b = d(r-ks)$

$\Rightarrow \underline{d \mid b}$

Let $d' = g.c.d.(b, n)$

$\Rightarrow d \leq d'$ $(\because d \mid b)$

Moreover, $d' \mid a$ ($\because$ similar reason as above)

$\Rightarrow d' \leq d = g.c.d(a, n)$

$\therefore \underline{d' = d}$

Ex!- Find remainders, when 2^{50} and 41^{65} are divided by 7.

$2^3 = 8 \equiv 1 \bmod 7$

$50 = 3 \times 16 + 2$

$\therefore \quad (2^3)^{16} \equiv 1 \bmod 7$

$\Rightarrow 2^{48} \equiv 1 \bmod 7$

$2^2 = 4 \equiv 4 \pmod 7$

$2^{50} = 2^{48} \cdot 2^2 \equiv 1 \times 4 \equiv 4 \pmod 7$

$\therefore$ 4 is the remainder when 2^{50} is divided by 7.

41^{65} when divided by 7:

$42 \equiv 0 \pmod 7 \Rightarrow 41 \equiv -1 \pmod 7$

$\therefore (41)^{65} \equiv (-1)^{65} \pmod 7$

$\therefore 41^{65} \equiv -1 \pmod 7$

But $-1 \equiv 6 \pmod 7$

$\therefore$ 6 is the remainder, when 41^{65} is divided by 7

Ex:- What is the remainder when the sum

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

is divisible by 4.?

Ans:-

$1 \equiv 5 \equiv 9 \equiv \ldots\ldots \equiv 97 \pmod 4$

$2 \equiv 6 \equiv 10 \equiv \ldots\ldots \equiv 98 \pmod 4$

$3 \equiv 7 \equiv 11 \equiv \ldots\ldots \equiv 99 \pmod 4$

$4 \equiv 8 \equiv \cdots\cdots \equiv 100 \pmod 4$

$$\begin{cases} 1^5 \equiv 1 \pmod 4 \\ 2^5 \equiv 32 \equiv 0 \pmod 4 \\ 3^5 \equiv (-1)^5 \equiv -1 \equiv 3 \pmod 4 \\ 4^5 \equiv 0 \pmod 4 \end{cases}$$

$\therefore (1^5 + 2^5 + 3^5 + 4^5) + (\cdots\cdots) + \cdots$

$+ (97^5 + 98^5 + 99^5 + 100^5)$

$\pmod 4$

$\Rightarrow (1 + 0 + 3 + 0) + (\cdots\cdots) + \cdots$

$+ (\cdots\cdots) + (1 + 0 + 3 + 0)$

$\pmod 4$

$\equiv 0 \pmod 4$

$\Rightarrow$ remainder $= \underline{0}$.

Ex:- Prove that $7 \mid 5^{2n} + 3 \cdot 2^{5n-2}$ for $n \geq 1$.

Proof:- $5^2 = 25 \equiv 4 \pmod 7$

$\Rightarrow 5^{2n} \equiv 4^n \pmod 7$

$2^5 = 32 \equiv 4 \pmod 7$

$2^{5n} \equiv 4^n \pmod 7$

$2^{5n-2} = 2^{5n} \cdot 2^{-2} = 2^{5n} \cdot 4^{-1}$

$\equiv 4^n \cdot 4^{-1} \pmod 7$

$\Rightarrow 2^{5n-2} \equiv 4^{n-1} \pmod 7$

$3 \cdot 2^{5n-2} \equiv 3 \cdot 4^{n-1} \pmod 7$

$\therefore 5^{2n} + 3 \cdot 2^{5n-2} \equiv 4^n + 3 \cdot 4^{n-1}$

$$\Rightarrow 5^{2n} + 3 \cdot 2^{5n-2} \equiv 4 \cdot 4^{n-1} + 3 \cdot 4^{n-1}$$

$$\equiv 7 \cdot 4^{n-1}$$

$$\equiv 0 \pmod 7$$

$$\therefore 7 \mid 5^{2n} + 3 \cdot 2^{5n-2}$$

Ex:- $13 \mid 3^{n+2} + 4^{2n+1}$

$$3 \equiv 16 \pmod{13}$$

$$3^n \equiv 4^{2n} \pmod{13}$$

$$3^{n+2} \equiv 4^{2n} \times 9 \pmod{13}$$

$$\Rightarrow 3^{n+2} + 4^{2n+1} \equiv 9 \times 4^{2n} + 4 \times 4^{2n}$$

$$\equiv 13 \times 4^{2n}$$

$$\equiv 0 \pmod{13}$$

$\therefore \quad 13 \mid 3^{n+2} + 4^{2n+1}$

(HW) $27 \mid 2^{5n+1} + 5^{n+2}$

$43 \mid 6^{n+2} + 7^{2n+1}$

Note :-

$$\left.\begin{aligned} a &\equiv b \pmod{n_1} \\ a &\equiv b \pmod{n_2} \end{aligned}\right\} \Rightarrow a \equiv b \pmod{n}$$

where

$n = l.c.m(n_1, n_2)$

In fact, $n_1 \mid a-b$ and $n_2 \mid a-b$

$\Rightarrow a - b = k_1 n_1$

$a - b = k_2 n_2$

Let $d = g.c.d.(n_1, n_2)$

$\Rightarrow n_1 = dq$ and $n_2 = ds$

(where $(q, s) = 1$)

$$\therefore a - b = k_2 n_2 = k_2 n_2 \left(\frac{n_1}{d_1}\right)$$

$$\left(\because \frac{n_1}{d_1} = 1\right)$$

$$\Rightarrow a - b = k_2 \frac{n_2 n_1}{d_1}$$

$$= \frac{k_2}{d_1}\left(\frac{n_2 n_1}{d}\right)$$

$$= \frac{k_2}{d_1}\left(\text{l.c.m.}(n_1, n_2)\right)$$

$$\left(\because (\text{l.c.m.})(\text{gcd}) = n_1 n_2\right)$$

$$= \frac{k_2}{d_1}(n)$$

To show that $\frac{k_2}{n}$ is integer.

$n_2 = ds$ and

$a - b = k_1 n_1 = k_2 n_2$

$\Rightarrow k_1 (dr) = k_2 (ds)$

$\Rightarrow k_1 r = k_2 s$

$\Rightarrow r \mid k_2 s$

$\Rightarrow r \mid k_2$ $(\because (r, s) = 1)$

$\Rightarrow \frac{k_2}{r}$ is integer.

Note!- If $ab \equiv cd \pmod{n}$, and $b \equiv d \pmod{n}$, with $(b, n) = 1$, then $a \equiv c \pmod{n}$

Proof:- $b \equiv d \pmod{n}$

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

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

$(\because cd \equiv ab \pmod{n})$

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

$(\because g.c.d.(b, n) = 1)$

Theorem:-

$ax \equiv b \pmod{n}$ has a solution if and only if $d \mid b$, where $d = g.c.d(a, n)$.

If $d \mid n$, then there are d mutually incongruent solutions modulo n.

*

Proof:- $ax \equiv b \pmod{n}$ has a solution $\Rightarrow n \mid ax - b$.

$$\Rightarrow ax - b = ny$$

$$\Rightarrow \underline{ax - ny = b}$$

This Diophantine equation is solvable if and only if $d = g.c.d.(a, n) \mid b$

Moreover, if x_0, y_0 is a particular solution, then general solution is

$$x = x_0 + \frac{n}{d}t \quad , \quad y = y_0 + \frac{a}{d}t$$

For $t = 0, 1, 2, \ldots, d-1$,

$$x = x_0, \; x_0 + \frac{n}{d}, \; x_0 + 2\frac{n}{d}, \ldots\ldots$$

$$x_0 + (d-1)\frac{n}{d}$$

are d solutions which are mutually incongruent

Note:- If g.c.d.$(a,n)=1$, then $ax \equiv b \pmod{n}$ has a unique solution.

Ex:- $25x \equiv 15 \pmod{29}$

Ans: $-4x \equiv -14 \pmod{29}$

$2x \equiv 7 \pmod{29}$

$(\because (2,29)=1)$

Now $30 \equiv 1 \pmod{29}$

$\Rightarrow 2 \times 15 \equiv 1 \pmod{29}$

$\Rightarrow 15 = 2^{-1} \pmod{29}$

$\Rightarrow x \equiv 7 \times 15 \pmod{29}$

$\Rightarrow \underline{x \equiv 18 \pmod{29}}$

Ex:- $5x \equiv 2 \pmod{26}$

$5 \times 5x \equiv 5 \times 2 \pmod{26}$

$25x \equiv 10 \pmod{26}$

$-x \equiv 10 \pmod{26}$

$\Rightarrow x \equiv -10 \pmod{26}$

$\Rightarrow \underline{x = 16 \pmod{26}}$

Ex:- $6x \equiv 15 \pmod{21}$

g.c.d. $(6, 21) = 3$ and $3 \mid 15$

$\Rightarrow$ 3 incongruent solutions.

$\Rightarrow \left(\frac{6}{3}\right)x = \left(\frac{15}{3}\right) \pmod{\frac{21}{3}}$

$\Rightarrow 2x \equiv 5 \pmod 7$

$\Rightarrow 3 \times 2x \equiv 3 \times 5 \pmod 7$

$\Rightarrow 6x \equiv 15 \pmod 7$

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

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

$\Rightarrow x \equiv 6 \pmod 7$

$\therefore x = 6, \quad 6+7, \quad 6+2\times 7$

$\Rightarrow$ 6, 13, and 20 are three incongruent solutions mod 21.

(HW) $36x \equiv 8 \pmod{102}$

$34x \equiv 60 \pmod{98}$

$140x \equiv 133 \pmod{301}$

Ex!- Use congruences to solve the Diophantine equation:

$$4x + 51y = 9$$

Ans: $4x \equiv 9 \pmod{51}$ → (1)

$51y \equiv 9 \pmod{4}$ → (2)

$$4x \equiv 9 \pmod{51}$$

$$13 \times 4x \equiv 13 \times 9 \pmod{51}$$

$$\Rightarrow 52x \equiv 117 \pmod{51}$$

$$\Rightarrow x \equiv 15 \pmod{51}$$

$$\therefore x = 15 + 51t$$

(2) $\Rightarrow 51y \equiv 9 \pmod{4}$

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

$$\Rightarrow -y \equiv 1 \pmod 4$$

$$\Rightarrow y \equiv -1 \pmod 4$$

$$\Rightarrow y \equiv 3 \pmod 4$$

$$\therefore y = 3 + 4s$$

$$\left.\begin{aligned} x &= 15 + 51t \\ y &= 3 + 4s \end{aligned}\right\} \Rightarrow$$

$$4x + 51y = 4(15 + 51t) + 51(3 + 4s)$$

$$= 60 + 204t + 153 + 204s$$

$$\Rightarrow 9 = 213 + 204t + 204s$$

$$\Rightarrow -204 = 204t + 204s$$

$$\Rightarrow t + s = -1$$

$\Rightarrow s = -1 - t$

$\therefore \left.\begin{aligned} x &= 15 + 51t \\ y &= 3 + 4(-1-t) \end{aligned}\right\} \Rightarrow$

$x = 15 + 51t$

$y = -1 - 4t$

(HW) $12x + 25y = 331$