Polynomial Congruence :-

Let, $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0 \quad (n \geq 1)$

be a polynomial with integer coeff.s $a_0, a_1, \ldots, a_n$ with $a_n \not\equiv 0 \pmod{m}$

then, $f(x) \equiv 0 \pmod{m}$ is said to be a Polynomial Congruence $(\mathrm{mod}\ m)$ of degree n.

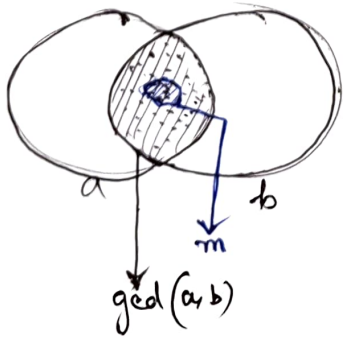
- If one solution be found, then infinitely many sol^{n}s can be obtained, but all these sol^{n}s belong to the same Residue class modulo m.
- Two sol^{n}s x_1 and x_2 are said to be distinct sol^{n}s, if $x_1 \not\equiv x_2 \pmod{m}$
- By number of sol^{n}s of Polynomial Congruence, we mean the number of incongruent (distinct) sol^{n}s.
- (*) There can not be more than m distinct sol^{n}s of the congruence, since there are only m different residue classes. If m is a small number, then it is easy to find all the distinct sol^{n}s by direct substitution,

$x = 1, \quad x = 2, \quad \ldots, \quad x = m-1$.

- **Difference between:**

Polynomial Congruence	Polynomial Equation
(i) A congruence may have no soln. Eg: $x^2 \equiv 3 \pmod 5$, which can be verified by checking for, $x = 1, 2, 3, 4$.	(i) A polynomial eqn has always a soln
(ii) A polynomial congruence may have more distinct soln's than its degree. Eg: $x^2 \equiv 1 \pmod 8$ has four distinct soln's: $x = 1, 3, 5, 7$.	(ii) A polynomial eqn of degree n has exactly n soln's.
(iii) There is an explicit method of solving a congruence of any degree modulo a positive integer $m > 1$, just by substituting each of the integers $1, 2, \ldots, m-1$, in turn.	(iii) There is no such explicit method for solving a polynomial eqn of degree > 4.

- If, $m \mid \gcd(a, b)$, then, $\dfrac{\gcd(a, b)}{m} = \gcd\left(\dfrac{a}{m}, \dfrac{b}{m}\right)$



Linear Congruence :~

A polynomial congruence of degree 1 is said to be a linear congruence.

General form : $ax \equiv b \pmod n$, with $a \not\equiv 0 \pmod n$

Theorem If x_1 be a sol^n of the congruence $ax \equiv b \pmod n$, then, $(x_1 + \lambda n)$ is also a sol^n, with $\lambda = 0, \pm 1, \pm 2, \ldots$ All these sol^{n}s belong to the same residue class modulo n.

- If x_0 be a sol^n of $ax \equiv b \pmod n$, then

$$ax_0 \equiv b \pmod n \iff n \mid (ax_0 - b)$$

or, $$ax_0 \equiv b \pmod n \iff \forall x_0 \exists y_0 (ax_0 - b = ny_0)$$

or, $$ax_0 \equiv b \pmod n \iff \forall x_0 \exists y_0 (ax_0 - ny_0 = b)$$

This is a linear Diophantine eq^n.

Theorem :~ The linear congruence $ax \equiv b \pmod n$ has a sol^n if and only if, $d \mid b$, where $d = \gcd(a, n)$. If $d \mid b$, then it has d mutually incongruent sol^{n}s modulo n.

Proof :— $ax \equiv b \pmod n$ is equivalent to the linear Diophantine eq^n $ax - ny = b$.

This is solvable if, $d \mid b$, and if x_0, y_0 is one specific sol^n, then any other sol^n is of the form:

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

Among the various soln's satisfying $x = x_0 + \frac{n}{d}t$, consider those that occur, when $t = 0, 1, 2, \ldots, d-1$,

i.e, $x_0, x_0 + \frac{n}{d}, x_0 + \frac{2n}{d}, \ldots, x_0 + \frac{(d-1)}{d}n$

We claim that these are incongruent modulo n, and all other such integers x are congruent to some one of them.

Proof: If it happened that, (t_1, t_2)

$x_0 + \frac{n}{d}t_1 \equiv x_0 + \frac{n}{d}t_2 \pmod{n}$, where, $0 \leq t_1 \leq t_2 \leq d-1$

then, $t_1 \equiv t_2 \pmod{\frac{n}{\gcd(\frac{n}{d}, n)}}$

or, $t_1 \equiv t_2 \pmod{\frac{n}{n/d}}$

or, $t_1 \equiv t_2 \pmod{d}$

$\Rightarrow d \mid (t_1 - t_2)$

But it contradicts that, $0 \leq t_1 \leq t_2 \leq d-1$

or, $t_1 - t_2 \leq d-1$

$\therefore$ So, $x_0 + \frac{n}{d}t_1 \not\equiv x_0 + \frac{n}{d}t_2 \pmod{n}$,

if, $0 \leq t_1 \leq t_2 \leq d-1$

Again, $x_0 + \frac{n}{d}t$ is congruent modulo n to one of the d integers listed above.

Proof:

By division algorithm, $t = qd + r$, $0 \leq r \leq d-1$,

$\therefore x_0 + \frac{n}{d}t = x_0 + \frac{n}{d}(qd + r)$

$\equiv x_0 + \frac{n}{d}r + nq \pmod{n}$

$\equiv x_0 + \frac{n}{d}r \pmod{n}$

, where, $0 \leq r \leq d-1$

∴ If x_0 is any sol^n of $ax \equiv b \pmod n$, then, the $d (= \gcd(a,n))$ incongruent solutions are:

$x_0,\ x_0 + \left(\frac{n}{d}\right),\ x_0 + 2.\left(\frac{n}{d}\right),\ \ldots,\ x_0 + (d-1).\left(\frac{n}{d}\right)$

Alternative proof of 2nd Part :-

$d \mid b$.

Let a sol^n be x_0.

$\therefore\ ax_0 \equiv b \pmod n$ (i) holds, if and only if,

$\frac{a}{d} x_0 \equiv \frac{b}{d} \pmod{\frac{n}{d}}$, where, $d = \gcd(a,n)$.

Now, $\gcd\left(\frac{a}{d}, \frac{n}{d}\right) = 1$

$\therefore$ (i) has only one sol^n.

In other words, the sol^n of the congruences $\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{n}{d}}$ are the integers congruent to x_0 mod $\frac{n}{d}$.

i.e, $x_0 + \frac{n}{d} \times t$, $t = 0, \pm 1, \pm 2, \ldots$

Now, between those sol^{n}s, those are incongruent modulo n, if we take, $t = 0, 1, 2, \ldots, d-1$,

i.e, $x_0, x_0 + \frac{n}{d}, x_0 + 2\frac{n}{d}, x_0 + 3\frac{n}{d} + \ldots, x_0 + (d-1)\left(\frac{n}{d}\right)$.

and all other sol^{n}s are incongruent modulo n. (Prove it)

Thus, $\left\{x_0, x_0 + \left(\frac{n}{d}\right), x_0 + 2.\left(\frac{n}{d}\right), \ldots, x_0 + (d-1)\left(\frac{n}{d}\right)\right\}$ are the distinct sol^{n}s for, $ax \equiv b \pmod n$.

Note

The sol^{n}s belong to a single residue class modulo $\frac{n}{d}$, i.e., the sol^{n}s are mutually congruent modulo $\frac{n}{d}$, and this single residue class is the union of d distinct residue classes modulo n.

- The residue class $\bar{i} \pmod{\frac{n}{d}}$ is the union of d distinct residue classes

$$\bar{i},\ \overline{i+\tfrac{n}{d}},\ \overline{i+2\cdot\tfrac{n}{d}},\ \ldots,\ \overline{i+(d-1)\left(\tfrac{n}{d}\right)} \pmod{n}$$

Eg:

Solve $3x \equiv 3 \pmod{15}$

$\Rightarrow 3x \equiv 3 \pmod{15}$

$\Rightarrow x \equiv 1 \pmod{5}$ $\quad \because d = \gcd(3,15) = 3,\ \therefore \frac{n}{d} = \frac{15}{3} = 5$

$\therefore x = x_0 + \left(\frac{n}{d}\right)t = 1 + 5t$

Now, for $t = 0, 1, 2$

$x = 1, 6, 11$ are the distinct sol^{n}s for $3x \equiv 3 \pmod{15}$

and, $\bar{1} \pmod 5 = \bar{1} \pmod{15} \cup \bar{6} \pmod{15} \cup \overline{11} \pmod{15}$

Corollary :~

If $\gcd(a, n) = 1$, then the linear congruence $ax \equiv b \pmod{n}$ has a unique sol^n modulo n.

Inverse :

Given relatively prime integers a and n, the congruence, $ax \equiv 1 \pmod{n}$ has a unique sol^n modulo n. This sol^n is called the multiplicative inverse of a modulo n.

Examples:

(1) Solve the linear congruence, $5x \equiv 3 \pmod{11}$. — (i)

→ Now, $\gcd(5, 11) = 1$,

∴ (i) has unique sol^n modulo 11.

Now, $\because \gcd(5, 11) = 1$,

∴ $\exists\ u, v$, s.t, $5u + 11v = 1$.

Now, $5(-2) + 11(1) = 1$

Or, $5 \times (-2) \equiv 1 \pmod{11}$

or, $5 \times (-6) \equiv 3 \pmod{11}$

∴ $x \equiv -6$ is a sol^n,

∴ All sol^n are, $x \equiv -6 \pmod{11}$,

i.e, $x \equiv 5 \pmod{11}$.

∴ All sol^{n}s are congruent to $5 \pmod{11}$.

∴ The given congruence has an unique sol^n.

(2) Solve, $15x \equiv 9 \pmod{18}$ ——— (i)

$\Rightarrow$ $\gcd(15, 18) = 3$ and, $3 \mid 9$

$\therefore$ (i) has 3 distinct sol^{n}s.

The given congruence is equivalent to,

$$\frac{15}{3}x \equiv \frac{9}{3} \pmod{\frac{18}{3}}$$

or, $5x \equiv 3 \pmod 6$ ——— (ii)

Now, $\gcd(5, 6) = 1$ $\therefore$ (ii) has unique sol^n mod 6.

and, $\exists\ u, v \in \mathbb{Z}$, s.t, $5u + 6v = 1$

Now, $5(-1) + 6(1) = 1$

or, $5(-1) = 6 + 1$

or, $5(-1) \equiv 1 \pmod 6$

or, $5(-3) \equiv 3 \pmod 6$

or, $5 \times 3 \equiv 3 \pmod 6$

$\therefore$ $x = 3$ is a sol^n of $5x \equiv 3 \pmod 6$.

$\therefore$ Therefore, the incongruent (distinct) sol^{n}s of $15x \equiv 9 \pmod{18}$ are : $\{3 + (\frac{n}{d}) \times t\}$ where, $t = 0, 1, 2, \ldots, (d-1)$

and, $n = 18$, $d = 3$.

i.e, $3, 3+6, 3+2\times6$.

i.e, $3, 9, 15$.

$\therefore$ The incongruent sol^{n}s are, $x \equiv 3, 9, 15 \pmod{18}$

Suppose, for, $ax \equiv b \pmod{n}$ has a sol^n.

and, $d = \gcd(a, n)$, $\therefore d \mid b$

Now, $\gcd\left(\frac{a}{d}, \frac{n}{d}\right) = 1$

Now, $\frac{a}{d} x \equiv \frac{b}{d} \pmod{\frac{n}{d}}$ has unique sol^n. modulo $\frac{n}{d}$.

and, $\left(\frac{a}{d}\right) u + \left(\frac{n}{d}\right) v = 1$ for some u and v

i.e, $\left(\frac{a}{d}\right) \cdot u = \left(\frac{n}{d}\right) v + 1$

i.e, $\left(\frac{a}{d}\right) u \equiv 1 \pmod{\frac{n}{d}}$

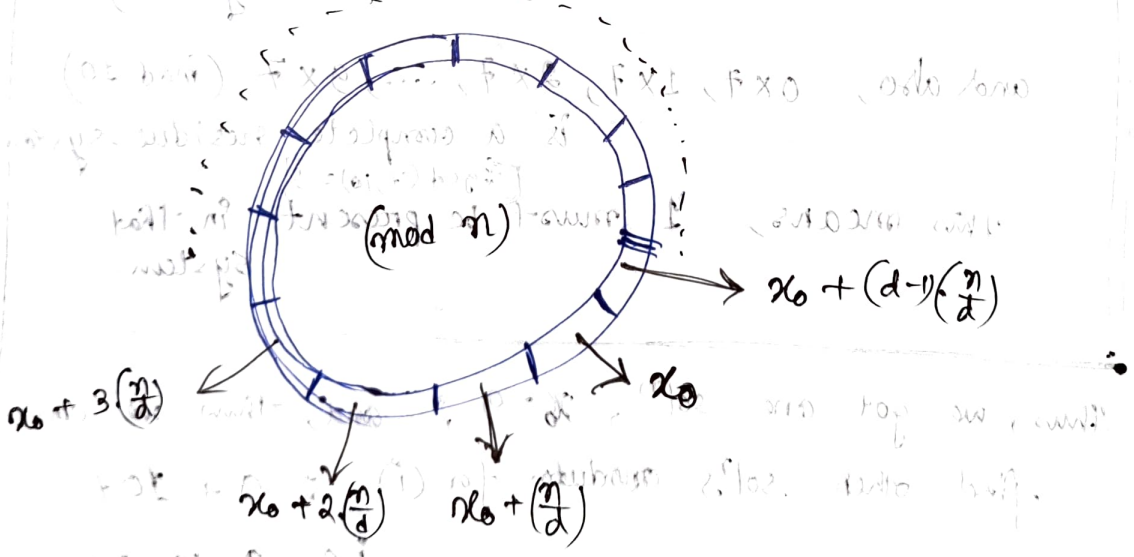
or, $\left(\frac{a}{d}\right) \cdot \left(u \times \frac{b}{d}\right) \equiv \frac{b}{d} \pmod{\frac{n}{d}}$

$\therefore \left(u \times \frac{b}{d}\right)$ is a sol^n of $ax \equiv b \pmod{n}$

or, $a x \left(u \times \frac{b}{d}\right) \equiv b \pmod{\frac{n}{d}}$

$\therefore x_0 = \left(u \times \frac{b}{d}\right)$ is a sol^n of $ax \equiv b \pmod{n}$

then, other sol^{n}s will be $x_0 + \frac{n}{d} \times t$, for $t = 0, 1, 2, \ldots, (d-1)$



(3) Solve : $9x \equiv 21 \pmod{30}$ ——— (i)

$\gcd(9, 30) = 3$, and , $3 \mid 21$

$\therefore$ $9x \equiv 21 \pmod{30}$ has sol^{n}s.

Now, The equivalent congruence is,

$3x \equiv 7 \pmod{10}$ ——— (ii)

The relative primeness of 3 and 10 implies that the later congruence admits an unique sol^n modulo 10.

Although it is not the most efficient method, we could test the integers $0, 1, 2, \ldots, 9$ in turn until the sol^n is obtained for (ii).

Multiplying the congruence by 7,

$21x \equiv 49 \pmod{10}$

i.e, $x \equiv 9 \pmod{10}$

This simplification is no accident.

Because $0, 1, 2, \ldots, 9 \pmod{10}$ is a complete residue system,

and also, $0\times7, 1\times7, 2\times7, \ldots, 9\times7 \pmod{10}$ is a complete residue system.

[$\because \gcd(7, 10) = 1$]

This means, 1 must be present in that system.

Thus, we got one sol^n, $x_0 = 9$, and, thus we can find other sol^{n}s for (i) : $9 + 10t$

i.e, 9, 19, 29.

A different approach: is to use the Diophantine eqn

$$9x - 30y = 21$$

Now, $\gcd(9, 30) = 3$. and, $3 \mid 21$

So we can express 3 as a linear combination of 9 and 30.

By Euclidean Algorithm, we can find, $3 = 9(-3) + 30$

$$\Rightarrow 9(-3) = -30 + 3$$

$$\Rightarrow 9 \times (-3) \equiv 3 \pmod{30}$$

$\therefore$ so that $21 = 3 \times 7 = 7 \times \{9(-3) + 30\}$

$$= 9(-21) + 30$$

or, $9(-21) = -30 + 21$

$\therefore$ $9(-21) \equiv 21 \pmod{30}$

or, $9 \times (9) \equiv 21 \pmod{30}$

$\therefore$ $x_0 \equiv 9 \pmod{30}$ is a soln.

$\therefore$ Other distinct soln's are, $x_0 = 9 + 10, 9 + 2 \times 10$

$\therefore$ All distinct soln's are:

$x \equiv 9, 19, 29 \pmod{30}$.

System of Linear Congruence :~

$$\left.\begin{aligned} a_1 x &\equiv b_1 \pmod{n_1} \\ a_2 x &\equiv b_2 \pmod{n_2} \\ &\vdots \\ a_r x &\equiv b_r \pmod{n_r} \end{aligned}\right\}$$ is called System of Linear Congruences

Let, $d_i = \gcd(a_i, n_i)$

The system will admit no sol^n unless each individual congruence is solvable, i.e, unless $d_i \mid b_i \ \forall\ i = 1(1)r$

If the system has simultaneous sol^n, i.e, $d_i \mid b_i$, cancelling d_i from the ith congruence, the system reduces to,

$a_1' x \equiv b_1' \pmod{n_1'}$, $a_2' x \equiv b_2' \pmod{n_2'}$, ...,

where, $d_i a_i' = a_i$, and, $d_i b_i' = b_i$, and, $d_i n_i' = n_i$,

and, $\gcd(a_i', n_i') = 1$

Each individual congruence has unique sol^n of the form, $x_i \equiv c_i \pmod{n_i'}$

Thus the problem is reduced to one of finding a common sol^n of the system :

$$\begin{aligned} x &\equiv c_1 \pmod{n_1'} \\ x &\equiv c_2 \pmod{n_2'} \\ &\vdots \\ x &\equiv c_r \pmod{n_r'} \end{aligned}$$

Chinese Remainder Theorem

Let, $n_1, n_2, \ldots, n_r$ be coprime integers $\left(\text{i.e, } \gcd(n_i, n_j) = 1 \;\; \forall\, i \neq j\right)$, then the system of linear congruences,

$$x \equiv b_1 \pmod{n_1}$$
$$x \equiv b_2 \pmod{n_2}$$
$$\vdots$$
$$x \equiv b_r \pmod{n_r}$$

has a simultaneous sol^n, which is unique modulo $(n_1, n_2, \ldots, n_r)$.

Proof :~

Let, $n = n_1 \cdot n_2 \cdot n_3 \ldots n_r$,

and, $N_i = \frac{n}{n_i} = n_1 n_2 \ldots n_{i-1} \cdot n_{i+1} \ldots n_r \;\; \forall\, i = 1(1)r$

In words, N_i is the product of all integers n_j, with the factor n_i omitted.

By hypothesis, the n_i are coprimes,

So, $\gcd(N_i, n_i) = 1$.

Now, $N_i x \equiv 1 \pmod{n_i}$ has unique sol^n because $\gcd(N_i, n_i) = 1$, (inverse of N_i)

and, let's call the unique sol^n x_i (multiplicative inverse of N_i modulo n_i)

Now, our aim is to prove this integer,

$$\bar{x} = b_1 N_1 x_1 + b_2 N_2 x_2 + \ldots + b_r N_r x_r$$

is a simultaneous sol^n of the given system.

First observe that, $N_j \equiv 0 \pmod{n_i}$ $\forall\ i \neq j$;

because, $n_i \mid N_j$ $\forall\ i \neq j$.

But the integer x_i was chosen to satisfy $N_i x_i \equiv 1 \pmod{n_i}$,

which forces, $\bar{x} \equiv b_i N_i x_i \pmod{n_i}$

or, $\bar{x} \equiv b_i \times 1 \pmod{n_i}$

or, $\bar{x} \equiv b_i \pmod{n_i}$ $\forall\ i = 1(1)r$,

$\Rightarrow$ This shows that $\bar{x}$ is a soln of the given system of congruence.

Now, we prove that this soln is unique;

Let, x' be any soln of the system.

$\therefore\ x' \equiv b_i \pmod{n_i}$ $\forall\ i = 1, 2, \ldots, r$

or, $x' \equiv \bar{x} \pmod{n_i}$ $\left[\because \bar{x} \equiv b_i \pmod{n_i}\right]$

Consequently,

$x' \equiv \bar{x} \pmod{n_1 . n_2 . n_3 \ldots n_r}$

$\therefore$ The soln of the system is unique modulo $n_1 . n_2 \ldots n_r$.

(Proved)

$\because\ x \equiv y \pmod{n_i}$ $\forall\ i = 1(1)r$

$\leftrightarrow\ x \equiv y \pmod{\text{lcm}(n_1, n_2, \ldots, n_r)}$

and, here in this case,

$\text{lcm}(n_1, n_2, \ldots, n_r) = \dfrac{n_1 . n_2 \ldots n_r}{\gcd(n_1, n_2, \ldots, n_r)}$

$= \dfrac{n_1 n_2 \ldots n_r}{1}$

The simultaneous soln of the system is,

$$\bar{x} = b_1 N_1 x_1 + b_2 N_2 x_2 + \ldots + b_r N_r x_r,$$

where, $N_i = \dfrac{n_1 . n_2 \ldots n_r}{n_i}$, and, x_i is the soln of $x \equiv b_i \pmod{n_i}$ $\forall\ i$

Alternate proof for uniqueness:

Let, x' be any other integer that satisfies these congruences.

$\therefore x \equiv b_i \equiv x' \pmod{n_i} \quad \forall\ i = 1, 2, \ldots, r$

$\therefore n_i \mid (x - x') \quad \forall\ i = 1, 2, \ldots, r$

$\therefore n_1 \mid (x - x')$
$n_2 \mid (x - x')$ and, $n_1, n_2, \ldots, n_r$ are coprimes.
$\vdots \quad \vdots \quad \vdots$
$n_r \mid (x - x')$

So, by Euclid's lemma, $n_1 \cdot n_2 \cdots n_r \mid (x - x')$

Example:

(1) Solve the system of linear congruence:

$x \equiv 1 \pmod 3, \quad x \equiv 2 \pmod 5, \quad x \equiv 3 \pmod 7$

$\Rightarrow$ 3, 5, 7 are pairwise coprimes.

So the system has an unique sol^n modulo $3.5.7$.

Let, $n = 3.5.7$

and, $N_1 = \frac{n}{3} = 35, \quad N_2 = \frac{n}{5} = 21, \quad N_3 = \frac{n}{7} = 15$

$\therefore$ we need to find the sol^{n}s of, $N_1 x \equiv 1 \pmod 3$, $N_2 x \equiv 1 \pmod 5$, $N_3 x \equiv 3 \pmod 7$

Now, $\gcd(N_1, 3) = 1, \quad \gcd(N_2, 5) = 1, \quad \gcd(N_3, 7) = 1$

$\therefore$ These congruences have unique sol^{n}s.

$\therefore$ the sol^{n}s are:

for, $35x \equiv 1 \pmod 3$, sol^n: $x_1 \equiv 2 \pmod 3$

for, $21x \equiv 1 \pmod 5$, sol^n: $x_2 \equiv 1 \pmod 5$

for, $15x \equiv 1 \pmod 7$, sol^n: $x_3 \equiv 1 \pmod 7$

The unique simultaneous soln of the given congruence system is:

$$\bar{x} \equiv \sum b_i N_i x_i \equiv 1\times 35\times 2 + 2\times 21\times 1 + 3\times 15\times 1 \pmod{3.5.7}$$

$$\equiv 70 + 42 + 45 \pmod{105}$$

$$\equiv 157 \pmod{105}$$

$$\therefore \bar{x} \equiv 52 \pmod{105}$$ Ans

---

(2) **Problem of Sun-Tsu:**

Find a number that leaves the remainders 2, 3, 2, when divided by 3, 5, 7 respectively.

This problem is equivalent to,

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

We have, $n = 3.5.7 = 105$

and, $N_1 = \frac{n}{3} = 35$, $N_2 = \frac{n}{5} = 21$, $N_3 = \frac{n}{7} = 15$

Now the linear congruences:

$$35x \equiv 1 \pmod 3, \quad 21x \equiv 1 \pmod 5, \quad 15x \equiv 1 \pmod 7$$

are satified by, $x_1 \equiv 2 \pmod 3$

$x_2 \equiv 1 \pmod 5$

$x_3 \equiv 1 \pmod 5$

∴ The soln of the system is:

$$\bar{x} \equiv 2\times 35\times 2 + 3\times 21\times 1 + 2\times 15\times 1 \pmod{105}$$

$$\equiv 140 + 63 + 30 \pmod{105}$$

$$\equiv 233 \pmod{105} \equiv 23 \pmod{105}$$

(3) ⭐⭐⭐⭐

Solve the linear combination $32x \equiv 79 \pmod{1225}$ by applying Chinese Remainder Theorem.

Now, $1225 = 5^2 \times 7^2$ and, $\gcd(5^2, 7^2) = 1$

The given problem is equivalent to finding a simultaneous soln of the congruence $32x \equiv 79 \pmod{5^2}$ and $32x \equiv 79 \pmod{7^2}$

Because,
$a \equiv b \pmod{n_1}$
and, $a \equiv b \pmod{n_2}$
$\leftrightarrow a \equiv b \pmod{\text{lcm}(n_1, n_2)}$

Now, $32x \equiv 79 \pmod{25}$
is equivalent to $7x \equiv 4 \pmod{25}$

Now, $\gcd(7, 25) = 1$, $\therefore$ This congruence has unique soln.

Now, $7 \times (-7) + 25 \times (2) = 1$

or, $7 \times (-7) \equiv 1 \pmod{25}$

or, $7 \times (-28) \equiv 4 \pmod{25}$

$\therefore x_1 \equiv -28 \pmod{25}$ is soln,

or, $x_1 \equiv -24 \times 3 \equiv 72 \equiv 22 \pmod{25}$

$\therefore x_1 \equiv 22 \pmod{25}$ ——— (i)

And, $32x \equiv 79 \pmod{49}$

or, $32x \equiv 30 \pmod{49}$, or, $16x \equiv 15 \pmod{49}$

Now, $\gcd(16, 49) = 1$, $\therefore$ This has unique soln.

Now, $16 \times (3) + 49 \times (+1) = 1$

or, $16 \times (3) \equiv 1 \pmod{49}$

or, $16 \times (45) \equiv 15 \pmod{49}$

$\therefore x_2 \equiv 45 \pmod{49}$ is a soln

(ii)

Now, from (i) and (ii),

We need to find a simultaneous sol^n

for, $x \equiv 22 \pmod{25}$

and, $x \equiv 4 \pmod{49}$

Now, $\gcd(25, 49) = 1$, $\therefore$ This system has sol^n.

Now, $n = 25 \times 49$

and, $N_1 = \frac{n}{25} = 49$, $N_2 = \frac{n}{49} = 25$

$\therefore$ for the congruence, $49x \equiv 1 \pmod{25}$

$\gcd(49, 25) = 1$

or, $49(-1) + 25(2) = 1$

or, $49(-1) \equiv 1 \pmod{25}$

$\therefore x \equiv -1 \pmod{25}$

$\therefore$ for the congruence, $25x \equiv 1 \pmod{49}$

$\gcd(25, 49) = 1$

or, $25(2) + 49(-1) = 1$

or, $25(2) \equiv 1 \pmod{49}$

$\therefore x \equiv 2 \pmod{49}$

$\therefore$ Simultaneous sol^n,

$$\bar{x} \equiv 22 \times 49 \times (-1) + 4 \times 25 \times 2 \pmod{25 \times 49}$$

$$\equiv -1078 + 200 \pmod{1225}$$

$$\equiv -878 \pmod{1225}$$

$\therefore \bar{x} \equiv 347 \pmod{1225}$

Ans

Alternative :~

For solving, $32x \equiv 79 \pmod{25}$

and, $32x \equiv 79 \pmod{49}$

i.e, $7x \equiv 4 \pmod{25}$ and, $32x \equiv 30 \pmod{49}$

for, $7x \equiv 4 \pmod{25}$, ——— (i)

$\gcd(7, 25) = 1$

$\therefore 7(-7) + 25(2) = 1$

or, $7x(-7) \equiv 1 \pmod{25}$

$\therefore$ Multiplying (i) with -7,

$7x(-7)x \equiv 4x(-7) \pmod{25}$

or, $1x \equiv -28 \pmod{25}$

or, $x \equiv 22 \pmod{25}$

$\therefore x = 22 + 25y$ ——— (ii)

$\therefore$ from (ii) and (iii),

$32(22 + 25y) \equiv 30 \pmod{49}$

or, $704 + 800y \equiv 30 \pmod{49}$

or, $18 + 16y \equiv 30 \pmod{49}$

or, $16y \equiv 12 \pmod{49}$

or, $4y \equiv 3 \pmod{49}$ ——— (iv)

Now, $\gcd(4, 49) = 1$

$\therefore 4x(-12) + 49(1) = 1$

or, $4x(-12) \equiv 1 \pmod{49}$

Multiplying (iv) by -12,

$\therefore 4y \equiv 3 \pmod{49}$

or, $4x(-12)xy \equiv -36 \pmod{49}$

or, $y \equiv 13 \pmod{49}$

$\therefore y = 13 + 49z$

$\therefore$ from (iii),

$x = 22 + 25(13 + 49z)$

$\Rightarrow x = 22 + 325 + (25 \times 49)z$

$\Rightarrow x = 347 + 1225z$

$\therefore x \equiv 347 \pmod{1225}$ (Ans)

---

(4) solve the linear congruence :

$17x \equiv 9 \pmod{276}$

⇒ Method 1 :—

By Euclid's Algorithm, we find $\gcd(17, 276)$

$\therefore 276 = 16 \times 17 + 4$

$17 = 4 \times 4 + 1$

$4 = 3 \times 1 + 1$

$1 = 1 \times 1 + 0$

$\therefore \gcd(276, 17)$
$= \gcd(17, 276 \% 17)$
$= \gcd(17, 4)$
$= \gcd(4, 17 \% 4)$
$= \gcd(4, 1) = 1$

Also 17 is prime and $17 \nmid 276$
$\therefore \gcd = 1$

$\therefore$ The congruence has unique soln.

Now, $\gcd(276, 17) = 1$

$= 4 - 3 \times 1$

$= 4 - 3 \times (17 - 4 \times 4)$

$= 4 - 3 \times 17 + 3 \times 4 \times 4$

$= 4 \times 13 - 3 \times 17$

$= 13(276 - 16 \times 17) - 3 \times 17$

$= 13 \times 276 - 17 \times (3 + 13 \times 16)$

$\therefore \quad 17 \times (-19) = -276 + 1$

or, $17 \times (-19) \equiv 1 \pmod{276}$

or, $17(-19 \times 9) \equiv 9 \pmod{276}$

$\therefore x \equiv -19 \times 9 \pmod{276}$

$\equiv -171 \pmod{276}$

or, $x \equiv 105 \pmod{276}$

171

276 | 171 | 105

16 × 13 = 48 + 16 = 208

$\therefore \quad 17x - (3 + 13 \times 16) = -13 \times 276 + 1$

or, $17x - (3 + 13 \times 16) \equiv 1 \pmod{276}$

or, $17x - 211 \equiv 1 \pmod{276}$

or, $17x - (211 \times 9) \equiv 9 \pmod{276}$

~~$17x - 1899 \equiv 9 \pmod{276}$~~

276 | 1899 | 6
1656
243

~~$\therefore x \equiv -1899 \pmod{276}$~~

$\therefore x \equiv -211 \times 9 \pmod{276}$

$\equiv 65 \times 9 \pmod{276}$

$\equiv 585 \pmod{276}$

276 | 585 | 2
552
33

or, $x \equiv 33 \pmod{276}$

is the solution.

Alternative :

$276 = 3 \times 4 \times 23$

$\therefore 17x \equiv 9 \pmod{276} \longleftrightarrow \begin{cases} 17x \equiv 9 \pmod 3 \\ 17x \equiv 9 \pmod 4 \\ 17x \equiv 9 \pmod{23} \end{cases}$

$\left[\because x \equiv a \pmod{n_i} \Leftrightarrow x \equiv a \pmod{\text{lcm}(n_1, n_2, \ldots, n_m)} \right]$

$\therefore$ The system of congruence is equivalent to :

$2x \equiv 0 \pmod 3$ ——— (i)

$x \equiv 1 \pmod 4$ ——— (ii)

$17x \equiv 9 \pmod{23}$ ——— (iii)

from (i), we get, $2x \equiv 0 \pmod 3$

or, $4x \equiv 0 \pmod 3$

or, $x \equiv 0 \pmod 3$

$\therefore x = 3k$ ——— (iv)

from (ii) and (iv),

$3k \equiv 1 \pmod 4$

or, $9k \equiv 3 \pmod 4$

or, $k \equiv 3 \pmod 4$

$\therefore k = 4j + 3$ ——— (v)

from (iv) and (v), $x = 12j + 9$ ——— (vi)

from (iii) and (vi),

$17(12j + 9) \equiv 9 \pmod{23}$

or, $204j + 153 \equiv 9 \pmod{23}$

or, $20j + 15 \equiv 9 \pmod{23}$

$\Rightarrow -20j \equiv 6 \pmod{23}$

$\Rightarrow 3j \equiv 6 \pmod{23}$

$\Rightarrow j \equiv 2 \pmod{23}$ $\quad [\because \gcd(3, 23) = 1]$

$\therefore$ from (vi), ~~$x = 24 + 276t$~~

$\therefore j = 2 + 23t$ ——— (vii)

From (vi), $x = 12(2 + 23t) + 9$

$= 24 + 276t + 9$

$= 33 + 276t$

$\therefore x \equiv 33 \pmod{276}$

is the soln. (Answer)

---

(5) Find four consecutive integers divisible by 3, 4, 5, 7 respectively.

⇒ Let, x, $x+1$, $x+2$, $x+3$ be four consecutive int.s.

Now, we need to solve the system :

$x \equiv 0 \pmod{3}$ ——— (i)

$x + 1 \equiv 0 \pmod{4}$, or, $x \equiv 3 \pmod{4}$ ——— (ii)

$x + 2 \equiv 0 \pmod{5}$, or, $x \equiv 3 \pmod{5}$ ——— (iii)

$x + 3 \equiv 0 \pmod{7}$, or, $x \equiv 4 \pmod{7}$ ——— (iv)

Now, 3, 4, 5, 7 are coprimes. So unique soln exists.

From (i), $x = 3K$ ——— (v)

From, (ii), $3K \equiv 3 \pmod{4}$, or, $K \equiv 1 \pmod{4}$

or, $K = 1 + 4j$ ——— (vi)

From

from (vi) $x = 3 + 12j$ ——— (vii)

from (iii), $3 + 12j \equiv 3 \pmod 5$

or, $12j \equiv 0 \pmod 5$

or, $36j \equiv 0 \pmod 5$

or, $j \equiv 0 \pmod 5$

$\therefore j = 5i$ ——— (viii)

From (vii), $x = 3 + 60i$ ——— (ix)

From, (iv), $x \equiv 4 \pmod 7$

or, $3 + 60i \equiv 4 \pmod 7$

or, $60i \equiv 1 \pmod 7$

or, $4i \equiv 1 \pmod 7$

or, $8i \equiv 2 \pmod 7$

or, $i \equiv 2 \pmod 7$

or, $i = 2 + 7t$ ——— (x)

from (vi) (ix) and (v),

$x = 3 + 60(2 + 7t)$

$= 3 + 120 + 420t$

$\therefore x \equiv 123 \pmod{420}$

Now, $n = 3 \cdot 4 \cdot 5 \cdot 7$
$= 420$

$\therefore$ Consecutive integers are, $x, x+1, x+2, x+3$,

when, $x \equiv 123 \pmod{420}$

Ans

Theorem :~

The system of linear congruences

$x \equiv c_1 \pmod{n_1}$ and, $x \equiv c_2 \pmod{n_2}$

will have a simultaneous sol^n, if and only if,

$\gcd(n_1, n_2) \mid (c_1 - c_2)$.

And if this cond^n is satisfied, the sol^n is unique modulo $\text{lcm}(n_1, n_2)$

Eg: (1) Solve the system :

$x \equiv 11 \pmod{15}$

$x \equiv 6 \pmod{35}$

Now, $\gcd(15, 35) = 5 \mid (11 - 6)$.

∴ This system has simultaneous sol^n.

Now, $x \equiv 11 \pmod{15} \Rightarrow x = 11 + 15K$ ——— (i)

and, $x \equiv 6 \pmod{35}$

$\Rightarrow 11 + 15K \equiv 6 \pmod{35}$

$\Rightarrow 15K \equiv -5 \equiv 30 \pmod{35}$

$\Rightarrow K \equiv 2 \pmod{\frac{35}{5}}$

$\Rightarrow K \equiv 2 \pmod{7}$.

∴ $K = 2 + 7s$

From (i) $\Rightarrow x = 11 + 15(2 + 7s) = 11 + 30 + 105s$

or, $x \equiv 41 \pmod{105}$ where, $105 = \text{lcm}(15, 35)$

(Ans)

Alternative :

$x \equiv 11 \pmod{15}$ [and, $15 = 3 \times 5$]

is equivalent to the system $\begin{cases} x \equiv 11 \pmod 3 \\ x \equiv 11 \pmod 5 \end{cases}$

and, $x \equiv 6 \pmod{35}$ [$35 = 5 \times 7$].

is equivalent to the system $\begin{cases} x \equiv 6 \pmod 5 \\ x \equiv 6 \pmod 7 \end{cases}$

Now, Thus the given system is equivalent to system of four simultaneous congruences :

$x \equiv 11 \pmod 3$, $x \equiv 11 \pmod 5$, $x \equiv 6 \pmod 5$, $x \equiv 6 \pmod 7$

Now, $x \equiv 11 \pmod 5$ and, $x \equiv 6 \pmod 5$ are consistent because, each is equivalent to, $x \equiv 1 \pmod 5$

Now, the modified system is :

$x \equiv 2 \pmod 3$
$x \equiv 1 \pmod 5$
$x \equiv 6 \pmod 7$

and, 3, 5, 7 are pairwise prime to each other,

(1) We can find sol^n of the system by Chinese Remainder theorem.

$n = 3 \times 5 \times 7 = 105$

$N_1 = \frac{n}{3} = 35$, $N_2 = \frac{n}{5} = 21$, $N_3 = \frac{n}{7} = 15$

$\therefore 35x \equiv 1 \pmod 3$, $21x \equiv 1 \pmod 5$, $15x \equiv 1 \pmod 7$ are satisfied by $x_1 = 2$, $x_2 = 1$, $x_3 = 1$

$\therefore$ The simultaneous sol^n is :

$$\bar{x} \equiv 2 \times 35 \times 2 + 1 \times 21 \times 1 + 6 \times 15 \times 1 \pmod{105}$$
$$\equiv 140 + 21 + 90 \pmod{105}$$
$$\equiv 251 \pmod{105}$$

or, $\bar{x} \equiv 41 \pmod{105}$

(2) Alt:
We could've also found the soln without Chinese Remainder Th. to solve:;

$x \equiv 2 \pmod 3$ ——— (i)
$x \equiv 1 \pmod 5$ ——— (ii)
$x \equiv 6 \pmod 7$ ——— (iii)

from, $x \equiv 2 \pmod 3$, $x = 2 + 3K$ ——— (iv)

from (ii), $2 + 3K \equiv 1 \pmod 5$
$\Rightarrow 3K \equiv 4 \pmod 5$
$\Rightarrow 6K \equiv 8 \pmod 5$
$\Rightarrow K \equiv 8 \pmod 5$
$\therefore K = 8 + 5s$ ——— (v)

from (iv) and (v); $x = 2 + 3(8 + 5s) = 2 + 24 + 15s$
$= 26 + 15s$ ——— (vi)

from (iii) and (vi), $26 + 15s \equiv 6 \pmod 7$
$\Rightarrow s \equiv 1 \pmod 7$
$\Rightarrow s = 1 + 7t$ ——— (vii)

From (vi) and (vii), $x = 26 + 15 + 105t$
$= 41 + 105t$

$\therefore$ soln is, $x \equiv 41 \pmod{105}$ (Ans)

Theorem :~

The system of linear congruences :

$$x \equiv a_1 \pmod{n_1}$$
$$x \equiv a_2 \pmod{n_2}$$
$$\vdots$$
$$x \equiv a_r \pmod{n_r}$$

will have simultaneous soln, if and only if,

$\gcd(n_i, n_j) \mid (a_i - a_j) \quad \forall \quad i \neq j$.

And if this cond^n is satisfied,
the sol^n is unique modulo $\text{lcm}(n_1, n_2, \ldots, n_r)$.

Eg: (1) The system : $x \equiv 2 \pmod 3$
$x \equiv 3 \pmod 5$
$x \equiv 4 \pmod 6$

has no sol^n, since $\gcd(3,6) \nmid (4-2)$.

Proof : Let, $\gcd(a,b,n) = \gcd(\gcd(a,b), n)$
$= \gcd(d_1, n) = d_2$

$\therefore \exists\ s, t \in \mathbb{Z}$, s.t, $d_1 s + nt = d_2$

and, $\because \gcd(a,b) = d_1$, $\therefore \exists\ u, v \in \mathbb{Z}$, s.t, $au + bv = d_1$

$\therefore$ $a(us) + b(vs) + n(t) = d_2$

$\therefore$ $d_2 = \gcd(a,b,n)$ can be expressed as a linear combination of a, b, n;
and d_2 is the least absolute value of all linear combinations among all the linear combination of a, b, n.

Now, $ax + by \equiv c \pmod n$ has a sol^n, means :
$ax + by - nz = c$

It's a linear combination of a, b, n. So, $\gcd(a,b,n) \mid (ax+by)$

$\therefore$ If $\gcd(a,b,n) \mid c$, then the congruence has sol^n.

Linear Congruence in two variables :

The congruence of the form : $ax + by \equiv c \pmod{n}$ has a soln, if and only if, $\gcd(a, b, n) \mid c$.

- The condition of solvability holds if, either $\gcd(a, n) = 1$ or, $\gcd(b, n) = 1$, i.e; n is relatively prime to one of a and b or both. Then, $\gcd(a, b, n) = 1$ will always divide c.

Now, say when, $\gcd(a, n) = 1$,

$$ax \equiv c - by \pmod{n}$$

will have an unique soln x for each of the n incongruent values of y.

Theorem :~ The system of linear congruence :

$$ax + by \equiv r \pmod{n} \quad \text{---(i)}$$
$$cx + dy \equiv s \pmod{n} \quad \text{---(ii)}$$

has unique soln modulo n, whenever, $\gcd(ad - bc, n) = 1$

This is similarly to solving two equations with two variables

Proof :~ (i) $\times d$ − (ii) $\times b \Rightarrow$ (i.e, Eliminating y)

$$(ad - bc)x \equiv dr - bs \pmod{n} \quad \text{---(iii)}$$

The assumption $\gcd(ad - bc, n) = 1$ ensures that (iii) has unique soln.

$\exists\ t$, s.t, $(ad - bc)t + n \cdot u = 1$

$n,\ (ad - bc)t \equiv 1 \pmod{n}$

(iii) $\times t \Rightarrow$ $x \equiv t(dr - bs) \pmod{n}$ → soln for x.

Similarly, from (i) and (ii), eliminating x, we get,

$y \equiv t(as - cr) \pmod{n}$ → soln for y

Example:

(1) Solve: $7x + 3y \equiv 10 \pmod{16}$ ——— (i)

$2x + 5y \equiv 9 \pmod{16}$ ——— (ii)

$\Rightarrow \gcd(7\times5 - 3\times2, 16) = \gcd(29, 16) = 1$

$\therefore$ The system has unique soln.

Eliminating y from (i) and (ii); i.e.,

(i) $\times 5$ − (ii) $\times 3 \Rightarrow$

$(35 - 6)x \equiv 23 \pmod{16}$

or, $29x \equiv 23 \pmod{16}$

or, $13x \equiv 7 \pmod{16}$

$\because \gcd(13, 16) = 1 \therefore$ This has unique soln.

$-3x \equiv -9 \pmod{16}$

or, $x \equiv 3 \pmod{16}$ ⟶ is a soln.

Now from (i),

$7\times3 + 3y \equiv 10 \pmod{16}$

or, $3y \equiv 5 \pmod{16}$

or, $3y \equiv 5 + 16 \equiv 21 \pmod{16}$

or, $y \equiv 7 \pmod{16}$ ⟶ 'y' a soln

$\therefore$ Ans: $x \equiv 3 \pmod{16}$ and, $y \equiv 7 \pmod{16}$.

Exercise (Page 83)

(1) a) Solve : $25x \equiv 15 \pmod{29}$

$\gcd(25, 29) = 1$ $\therefore$ Unique soln.

$\Rightarrow 5x \equiv 3 \pmod{29}$

Now, $\gcd(5, 29) = 1$

$\therefore 5 \times (6) + 29(-1) = 1$

$\Rightarrow 5 \times (6) \equiv 1 \pmod{29}$

$\Rightarrow 5 \times (18) \equiv 3 \pmod{29}$

$\therefore x \equiv 18 \pmod{29}$ is soln

(b) Solve : $5x \equiv 2 \pmod{26}$

$\Rightarrow \gcd(5, 26) = 1$ $\therefore$ Unique soln,

$5 \times (5) + 26 \times 1 = 1$

$\Rightarrow 5 \times (-5) \equiv 1 \pmod{26}$

$\Rightarrow 5 \times (-10) \equiv 2 \pmod{26}$

$\therefore x \equiv -10 \equiv 16 \pmod{26}$ (Ans)

(c) $6x \equiv 15 \pmod{21}$

$\Rightarrow \gcd(6, 21) = 3 \mid 15$ $\therefore$ 3 soln's exists.

$\therefore$ ~~$x \equiv 15 \pmod{21}$~~

$6 \times (-3) + 21 = 3$

$\Rightarrow 6 \times (-3) \equiv 3 \pmod{21}$

$\Rightarrow 6 \times (-15) \equiv 15 \pmod{21}$

$\therefore x \equiv -15 \pmod{21}$ is a soln.

$\therefore$ Other soln's are,

$x \equiv -15 + \frac{21}{3}$, $x \equiv -15 + 2 \cdot \frac{21}{3} \pmod{21}$

$\Rightarrow x \equiv 13$, $x \equiv 20 \pmod{21}$

$\therefore$ All soln's : $x \equiv 6, 13, 20 \pmod{21}$

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

$\Rightarrow \gcd(36, 102) = \gcd(36, 30) = 6 \nmid 8$

$\therefore$ No sol^n.

(e) $34x \equiv 60 \pmod{98}$

$\Rightarrow \gcd(34, 98) = \gcd(34, 30) = 2 \mid 60$

$\therefore$ 2 sol^{n}s exist.

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

$\Rightarrow 17x \equiv 30 \pmod{49}$

$\gcd(17, 49) = 1$

$\therefore 17 \times (-8) + 49 \times (3) = 1$

$\Rightarrow 17 \times (-8) \equiv 1 \pmod{49}$

$\Rightarrow 17 \times (-8 \times 30) \equiv 30 \pmod{49}$

$\therefore x \equiv -240 \pmod{49}$ is a soln

$\equiv 5 \pmod{49}$

$\therefore$ other soln is:

$x \equiv 5 + 49 \pmod{98}$

$\equiv 54 \pmod{98}$

Euclid's Alg.

$49 = 2 \times 17 + 15$

$17 = 1 \times 15 + 2$

$15 = 7 \times 2 + 1$

$2 = 2 \times 1 + 0$

Now, $1 = 15 - 7 \times 2 = 15 - 7 \times (17 - 15)$

$= 15 - 7 \times 17 + 7 \times 15$

$= 8 \times 15 - 7 \times 17$

$= 8 \times (49 - 2 \times 17) - 7 \times 17$

$= 8 \times 49 - 23 \times 17$

$\therefore$ $17x(-23) \equiv 1 \pmod{49}$

or, $17x(26) \equiv 1 \pmod{49}$

$\therefore x \equiv 26 \pmod{49}$ is a soln.

Other soln is : $x \equiv 26 + 49 \pmod{98}$

$\equiv 75 \pmod{98}$

a, $17x(26 \times 30) \equiv 30 \pmod{49}$

$49 \mid 780 \mid 16$
49
290
294
-4

or, $17x(45) \equiv 30 \pmod{49}$

$\therefore x \equiv 45 \pmod{49}$ is a soln.

Other soln : $x \equiv 45 + 49 \pmod{49}$

$\equiv 94 \pmod{49}$

These two soln are incongruent modulo 98.

$\therefore x \equiv 45, 94 \pmod{98}$ (Ans)

(f) $140x \equiv 133 \pmod{301}$

$140 \mid 301 \mid 2$
280
21

$\Rightarrow \gcd(140, 301) = \gcd(140, 21)$

$= \gcd(21, 14)$

$21 \mid 140 \mid 6$
126
14

$= 7$

and, $7 \mid 133$ $\therefore$ 7 soln's exist.

Now, $7 = 21 - 14 = 21 - (140 - 21 \times 6)$

$= 7 \times 21 - 140$

$= 7 \times (301 - 140 \times 2) - 140 = 7 \times 301 - 15 \times 140$

$\therefore 140x(-15) = 7 + 7 \times 301$

$\equiv 7 \pmod{301}$

or, $140x(-15x19) \equiv 7x19 \pmod{301}$

or, $140x(-285) \equiv 133 \pmod{301}$

~~or, $140x(15) \equiv 133 \pmod{301}$~~

$19 \times 15 = 95 + 190 = 285$

or, $140x(16) \equiv 133 \pmod{301}$

$\therefore x \equiv 16 \pmod{301}$ is a soln

$\therefore$ ~~All~~ soln's are : $\left[\frac{n}{d} = \frac{301}{7} = 43\right]$

~~$x \equiv 16 + 301$~~

$x \equiv 16, 16+43, 16+2.43, 16+3.43, 16+4.43, 16+5.43, 16+6.43 \pmod{301}$

or, $x \equiv 16, 59, 102, 145, 188, 231, 274 \pmod{301}$

Ans

---

(2) Using congruence, solve the Diophantine eqn:

(a) $4x + 51y = 9$ ——— (i)

$\Rightarrow 4x \equiv 9 \pmod{51}$ and, $51y \equiv 9 \pmod{4}$

or, $(4x13)x \equiv 9x13 \pmod{51}$ | or, $-y \equiv 1 \pmod{4}$

or, $52x \equiv 9x13 \pmod{51}$ | or, $y \equiv 3 \pmod{4}$

or, $x \equiv 117 \pmod{51}$

or, $x \equiv 15 \pmod{51}$

$\therefore x = 15 + 51s$ ——— (ii) | and, $y = 3 + 4t$ ——— (iii)

from (i); $60 + 204s + 153 + 204t = 9$

or, $204(s+t) = 9 - 213 = -204$

or, $s = -1 - t$ ——— (iv)

from (ii), $x = 15 - 51 - 51t = -36 - 51t$

∴ Soln : $x = -36 - 51t$, $y = 3 + 4t$

$= -36 - 51(-t' - 1)$ $= 3 + 4(-t' - 1)$

$= -36 + 51 + 51t'$ $= 3 - 4t' - 4$

or, $x = 15 + 51t'$ $= -1 - 4t'$

(Am)

---

(1)

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

$12x \equiv 331 \pmod{25}$ | $25y \equiv 331 \pmod{12}$

or, $24x \equiv 662 \pmod{25}$ | or, $y \equiv 7 \pmod{12}$

or, $x \equiv 12 \pmod{25}$

or, $x \equiv 12 \pmod{25}$ | ∴ $y = 7 + 12t$

∴ $x = 12 + 25s$

∴ from (1),

$12(12 + 25s) + 25(7 + 12t) = 331$

or, $144 + 300s + 175 + 300t = 331$

or, $300(s + t) = 12$

or, $25s = 1 - 25t$

∴ $x = 12 + 1 - 25t$

$x = 13 - 25t$ and, $y = 7 + 12t$

(Am)

12 | 14
13 | 12
24 | 14 | 8
12
14 4

25 | 12
50
25 0

3 3 3
3 3 1
1 2

331
319
12

(2) $5x - 53y = 17$

$\Rightarrow 5x \equiv 17 \pmod{53}$

~~$70x \equiv (17 \times 14) \pmod{53}$~~

$\Rightarrow 105x \equiv 17 \times 21 \pmod{53}$

$\Rightarrow -x \equiv 39 \pmod{53}$

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

$\therefore x = 14 + 53s$

$53y \equiv -17 \pmod{5}$

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

$\Rightarrow y \equiv 1 \pmod{5}$

$\therefore y = 1 + 5t$

$\therefore 5(14 + 53s) - 53(1 + 5t) = 17$

$\Rightarrow (53s - 53t) \times 5 = 17 - 70 + 53$

$= 0$

$\Rightarrow s = t$

$\therefore x = 14 + 53t$ and, $y = 1 + 5t$ Ans

(3) Find all sol^{n}s of the linear congruence:

$3x - 7y \equiv 11 \pmod{13}$

$\Rightarrow \gcd(3, 7, 13) = 1$

$\therefore$ This has ~~unique~~ sol^n.

Now, $3x \equiv 11 + 7y \pmod{13}$

and, $\gcd(3, 13) = 1$, ~~so there are~~ and $1 \mid (11 + 7y)$.

So there are 13 incongruent possibilities for $y \ (\equiv 0, 1, 2, \ldots, 12)$.

Now, $3x \equiv 11 + 7y \pmod{13}$

$\Rightarrow 27x \equiv 99 + 63y \pmod{13}$

$\Rightarrow x \equiv 8 + 11y \pmod{13}$

For, $y \equiv 0$:-

$3x \equiv 11 \pmod{13}$

$27x \equiv 99 \pmod{13}$

or, $x \equiv 8 \pmod{13}$

for, $y \equiv 1$:-

$x \equiv 19 \pmod{13}$

or,

$\therefore$ The soln's are :

(1) $y \equiv 0$, and, $x \equiv 8 \pmod{13}$

(2) $y \equiv 1$, and, $x \equiv 19 \equiv 6 \pmod{13}$

(3) $y \equiv 2$, and, $x \equiv 30 \equiv 4 \pmod{13}$

(4) $y \equiv 3$, and, $x \equiv 41 \equiv 2 \pmod{13}$

(5) $y \equiv 4$, and, $x \equiv 52 \equiv 0 \pmod{13}$

(6) $y \equiv 5$, and, $x \equiv 63 \equiv 11 \pmod{13}$

(7) $y \equiv 6$, and, $x \equiv 74 \equiv 9 \pmod{13}$

(8) $y \equiv 7$, and, $x \equiv 85 \equiv 7 \pmod{13}$

(9) $y \equiv 8$, and, $x \equiv 96 \equiv 5 \pmod{13}$

(10) $y \equiv 9$, and, $x \equiv 107 \equiv 3 \pmod{13}$

(11) $y \equiv 10$, and, $x \equiv 118 \equiv 1 \pmod{13}$

(12) $y \equiv 11$, and, $x \equiv 129 \equiv -1 \equiv 12 \pmod{13}$

(13) $y \equiv 12$, and, $x \equiv 140 \equiv 10 \pmod{13}$

Alternative : $3x - 7y \equiv 11 \pmod{13}$ ——— (i)

Now, $\gcd(3, 7) = 1$

and, $3(-2) + 7(1) \equiv 1$

or, $3(-22) + 7(-11) = 11$

$\therefore 3(-22) - 7(-11) \equiv 11 \pmod{13}$

$\therefore x_0 \equiv -22 \pmod{13}$, $y_0 \equiv -11 \pmod{13}$ is a soln.

$\therefore$ Similar to solving Diophantine equations :-

General soln's :

$x \equiv x_0 + \frac{b}{d}t \pmod{13}$ and, $y \equiv y_0 - \frac{a}{d}t \pmod{13}$

$\equiv -22 - 7t \pmod{13}$ $\equiv -11 - 3t \pmod{13}$

$\equiv 4 - 7t \pmod{13}$ $\equiv 2 - 3t \pmod{13}$

(Ans) (Ans)

Boi ei
Answer melate cheile,
$t = -1 - 2t'$ dhoro!

...ve each of the following sets of simultaneous linear congruences:

(c) $x \equiv 5 \pmod 6$, $x \equiv 4 \pmod{11}$, $x \equiv 3 \pmod{17}$

$\Rightarrow$ 6, 11, 17 are pairwise coprimes.

$\therefore$ Unique sol^n exists

$x \equiv 5 \pmod 6$

$\therefore x = 5K$

$x \equiv 4 \pmod{11}$

$\Rightarrow 5K \equiv 4 \pmod{11}$

$\Rightarrow 10K \equiv 8 \pmod{11}$

$\Rightarrow -K \equiv 8 \pmod{11}$

$\Rightarrow K \equiv 3 \pmod{11}$

$\therefore K = 3 + 11s$

$\therefore x = 15 + 55s$

$x \equiv 3 \pmod{17}$

$\Rightarrow 15 + 55s \equiv 3 \pmod{17}$

$\Rightarrow 45 \equiv 5 \pmod{17}$

$\Rightarrow 16s \equiv 20 \pmod{17}$

$\Rightarrow -s \equiv 3 \pmod{17}$

$\Rightarrow s \equiv 14 \pmod{17}$

$\Rightarrow s = 14 + 17t$

$\therefore x \equiv 15 + 55(14 + 17t) \pmod{}$

$= 15 + 770 + 55 \times 17t$

55
14
220
55×
770

---

(4) Solve each of the following sets of simultaneous linear congruence.

(c) $x \equiv 5 \pmod 6$, $x \equiv 4 \pmod{11}$, $x \equiv 3 \pmod{17}$

$\Rightarrow$ 6, 11, 17 are pairwise primes.

$\therefore$ Unique sol^n exists.

$x \equiv 5 \pmod 6$

$\Rightarrow x \equiv -1 \pmod 6$

$\Rightarrow x = 6K - 1$

$= 66s - 7$

$x \equiv 4 \pmod{11}$

$\Rightarrow 6K \equiv 5 \pmod{11}$

$\Rightarrow K \equiv 10 \pmod{11}$

$\Rightarrow K \equiv -1 \pmod{11}$

$\therefore K = 11s - 1$

$x \equiv 3 \pmod{17}$

$\Rightarrow 66s \equiv 10 \pmod{17}$

$\Rightarrow 15s \equiv 10 \pmod{17}$

$\Rightarrow 3s \equiv 2 \pmod{17}$

$\Rightarrow 3 \equiv 12 \pmod{17}$

$\Rightarrow s \equiv -5 \pmod{17}$

$\therefore s \equiv 17t - 5$

$\therefore x = 66(17t - 5) - 7$

$= 66 \times 17t - 330 - 7$

$\equiv -337 \pmod{6.11.17}$

$17 \times 6 = 102$, $102 + 17 = 119$, $119 \times 6 = 1122$

or, $x \equiv -337 \pmod{1122}$

$\therefore \boxed{x \equiv 785 \pmod{1122}}$ Solution)

(d) Solve : $2x \equiv 1 \pmod 5$, $3x \equiv 9 \pmod 6$,

$4x \equiv 1 \pmod 7$, $5x \equiv 9 \pmod{11}$

$\Rightarrow$ $2x \equiv 1 \pmod 5$: $-x \equiv 2$, or, $x \equiv 3 \pmod 5$

$3x \equiv 9 \pmod 6$: $x \equiv 3 \pmod 2$

$4x \equiv 1 \pmod 7$: $8x \equiv 2$, or, $x \equiv 2 \pmod 7$

$5x \equiv 9 \pmod{11}$: $10x \equiv 18$, or, $x \equiv 4 \pmod{11}$

Now, 5, 2, 7, 11 are pairwise coprimes.

So, unique soln exists.

Now, $n = 2.5.7.11 = 770$

$N_2 = \frac{n}{2} = 385$, $N_1 = \frac{n}{5} = 154$, $N_3 = \frac{n}{7} = 110$,

$N_4 = \frac{n}{11} = 70$

Now,

$154 x_1 \equiv 1 \pmod 5$	$385 x_2 \equiv 1 \pmod 2$
or, $x_1 \equiv 4 \pmod 5$	or, $x_2 \equiv 1 \pmod 2$
$110 x_3 \equiv 1 \pmod 7$	$70 x_4 \equiv 1 \pmod{11}$
or, $x_3 \equiv 3 \pmod 7$	or, $x_4 \equiv 3 \pmod{11}$

$\therefore$ Simultaneous soln :

$x \equiv 3 \times 154 \times 4 + 3 \times 385 \times 1 + 2 \times 110 \times 3 + 4 \times 70 \times 3 \pmod{770}$

$\equiv 4503 \equiv 653 \pmod{770}$ (Ans)

(5) Solve the linear congruence $17x \equiv 3 \pmod{2.3.5.7}$ by solving the system:

$17x \equiv 3 \pmod 2$ $\quad$ $17x \equiv 3 \pmod 3$

$17x \equiv 3 \pmod 5$ $\quad$ $17x \equiv 3 \pmod 7$

$\Rightarrow \text{lcm}(2,3,5,7) = 2.3.5.7$

$\therefore 17x \equiv 3 \pmod{2.3.5.7}$ is equivalent to the given system.

Now, 2, 3, 5, 7 are pairwise coprimes, so unique soln exists.

$\therefore 17x \equiv 3 \pmod 2 : x \equiv 3 \pmod 2$

$17x \equiv 3 \pmod 3 : 2x \equiv 3 \pmod 3$, or, $x \equiv 0 \pmod 3$

$17x \equiv 3 \pmod 5 : 2x \equiv 3 \pmod 5$, or, $x \equiv 4 \pmod 5$

$17x \equiv 3 \pmod 7 : 3x \equiv 3 \pmod 7$, or, $x \equiv 1 \pmod 7$

Now, $n = 2.3.5.7 = 210$

$N_1 = 105,\ N_2 = 70,\ N_3 = 42,\ N_4 = 30$

$\therefore 105\, x_1 \equiv 1 \pmod 2$	$70\, x_2 \equiv 1 \pmod 3$
or, $x_1 \equiv 1 \pmod 2$	or, $x_2 \equiv 1 \pmod 3$
$42\, x_3 \equiv 1 \pmod 5$	$30\, x_4 \equiv 1 \pmod 7$
or, $x_3 \equiv 3 \pmod 5$	or, $2x_4 \equiv 1 \pmod 7$
	or, $x_4 \equiv 4 \pmod 7$

$\therefore$ Simultaneous soln:

$$\bar{x} \equiv \sum c_i N_i x_i$$

or, $\bar{x} \equiv 3 \times 105 \times 1 + 0 \times 70 \times 1 + 4 \times 42 \times 3 + 1 \times 30 \times 4 \pmod{210}$

or, $\bar{x} \equiv 315 + 404 + 120 \pmod{210}$

$\equiv 839 \pmod{210} \equiv 209 \pmod{209}$

(6) Find the smallest integer $a > 2$, s.t.,

$2 \mid a$, $3 \mid a+1$, $4 \mid a+2$, $5 \mid a+3$, $6 \mid a+4$

⇒ This problem is equivalent to the system:

$x \equiv 0 \pmod 2$ or, $x \equiv 2 \pmod 2$

$x \equiv -1 \pmod 3$: or, $x \equiv 2 \pmod 3$

$x \equiv -2 \pmod 4$, or, $x \equiv 2 \pmod 4$

$x \equiv -3 \pmod 5$ or, $x \equiv 2 \pmod 5$

$x \equiv -4 \pmod 6$, or, $x \equiv 2 \pmod 6$

This system is equivalent to :

$x \equiv 2 \pmod{\text{lcm}(2,3,4,5,6)}$

or, $x \equiv 2 \pmod{60}$

$\therefore x = 2 + 60t$

Now, the smallest sol$^n > 2$ is 62 (Ans)

---

(7) (a) Obtain three consecutive integers, each having a square factor.

Hint: for sake of simplicity, find a, s.t.:

$2^2 \mid a$, $3^2 \mid a+1$, $5^2 \mid a+2$.

$\because 2^2, 3^2, 5^2$ are pairwise coprime

⇒ Equivalent system:

$a \equiv 0 \pmod 4$

$a \equiv -1 \pmod 9$

$a \equiv -2 \pmod{25}$

$\because$ 4, 9, 25 are pairwise prime,

$\therefore$ It's solvable

Let, $n = 4.9.25 = 900$

and, $N_1 = 225$, $N_2 = 100$, $N_3 = 36$

$\therefore 225 x_1 \equiv 1 \pmod 4$ | $100 x_2 \equiv 1 \pmod 9$ | $36 x_3 \equiv 1 \pmod{25}$

$\Rightarrow x_1 \equiv 1 \pmod 4$ | $\Rightarrow x_2 \equiv 1 \pmod 9$ | ~~$\Rightarrow x_3 \equiv 1 \pmod 5$~~

$\Rightarrow 11 x_3 \equiv 1 \pmod{25}$

$\Rightarrow 22 x_3 \equiv 2 \pmod{25}$

$\Rightarrow -3 x_3 \equiv 2 \pmod{25}$

$\Rightarrow 3x_3 \equiv -2 \pmod{25}$

$\Rightarrow 24 x_3 \equiv -16 \pmod{25}$

$\Rightarrow x_3 \equiv 16 \pmod{25}$

$\therefore$ Simultaneous sol^n:

$x \equiv \sum c_i N_i x_i$

$\equiv 0 - 1 \times 100 \times 1 - 2 \times 36 \times 16 \pmod{900}$

$\equiv -1252 \pmod{900}$

$\equiv -352 \equiv 548 \pmod{900}$

$\therefore$ one of the required set of three numbers is : $\{548, 549, 550\}$,

where, $2^2 | 548$, $3^2 | 549$,

$5^2 | 550$

Caution :

Note : $\gcd(36, 25) = 1$

$36x \equiv 1 \pmod{25}$ [This congruence has unique sol^n]

$\Rightarrow 11x \equiv 1 \pmod{25}$ [" " " "]

$\Rightarrow 5 \times 11 x \equiv 5 \pmod{25}$ [But, $\gcd(5, 25) = 5$, this congruence has 5 distinct sol^{n}s]

So, we can not multiply with a number c in both sides of $ax \equiv b \pmod n$, if $\gcd(c, n) > 1$, because this step will increase the number of sol^{n}s of the congruence

(b) Obtain three consecutive integers, the first of which is divisible by a square, the second by a cube, and the third by a fourth power.

⇒ consider: $x \equiv 0 \pmod{5^2}$
$x+1 \equiv 0 \pmod{3^3}$
$x+2 \equiv 0 \pmod{2^4}$

[chose reverse order to get smaller soln]

Equivalent to: $x \equiv 0 \pmod{25}$
$x \equiv -1 \pmod{27}$
$x \equiv -2 \pmod{16}$

Now, 25, 27, 16 are pairwise coprimes.
so unique soln exists.

Let, $n = 25.27.16 = 10800$
and, $N_2 = 400$, $N_3 = 675$

[We don't need to evaluate N_1 or, x_1, because, $a = 0$]

$\therefore 400 x_2 \equiv 1 \pmod{27}$
or, $-5x_2 \equiv 1 \pmod{27}$
or, $-25x_2 \equiv 5 \pmod{27}$
or, $2x_2 \equiv 5 \pmod{27}$
or, $28x_2 \equiv 5 \times 14 \pmod{27}$
or, $x_2 \equiv 16 \pmod{27}$
or, $x_2 \equiv -11 \pmod{27}$

$675 x_3 \equiv 1 \pmod{16}$
or, $3x_3 \equiv 1 \pmod{16}$
or, $15x_3 \equiv 5 \pmod{16}$
or, $x_3 \equiv -5 \pmod{16}$

$\therefore$ Simultaneous soln =

$$x \equiv \sum a_i N_i x_i \equiv 0 + (-1) \times 400 \times (-11) + (-2) \times 675 \times (-5)$$
$$\equiv 11,150 \pmod{10,800}$$
$$\equiv 350 \pmod{10,800}$$

$\therefore$ One soln is: {350, 351, 352}, where,
$5^2 | 350$, $3^3 | 351$, $2^4 | 352$ (Ans)

(8) (Brahmagupta, 7th century A.D.):

When eggs in a basket are removed 2, 3, 4, 5, 6 at a time, there remain respectively 1, 2, 3, 4, 5 eggs. When they are taken 7 at a time, none are left over. Find the smallest number of eggs that could have been contained in the basket.

⇒ Here, the problem is equivalent to the system of linear congruence:

$x \equiv 1 \pmod 2$, or, $x \equiv -1 \pmod 2$ —— (i)

$x \equiv 2 \pmod 3$, or, $x \equiv -1 \pmod 3$ —— (ii)

$x \equiv 3 \pmod 4$, or, $x \equiv -1 \pmod 4$ —— (iii)

$x \equiv 4 \pmod 5$, or, $x \equiv -1 \pmod 5$ —— (iv)

$x \equiv 5 \pmod 6$, or, $x \equiv -1 \pmod 6$ —— (v)

$x \equiv 0 \pmod 7$, or, $x \equiv 0 \pmod 7$ —— (vi)

The equivalent congruence of (i), (ii), (iii), (iv) and (v) is:

$x \equiv -1 \left(\text{mod } \text{lcm}(2, 3, 4, 5, 6)\right)$

or, $x \equiv -1 \pmod{60}$ —— (vii)

and, $x \equiv 0 \pmod 7$ —— (vi)

Now, $\gcd(7, 60) = 1$, ∴ (vi) and (vii) has unique soln

or, $x = 7K$ —— (viii)

∴ From (vii), $7K \equiv -1 \pmod{60}$

Now, $\gcd(7, 60) = 1$

Extended Euclid's Algorithm:

$60 = 7 \times (8) + 4$

$7 = 4 \times (1) + 3$

$4 = 3 \times (1) + 1$

$3 = 1 \cdot (3) + 0$

$\therefore 1 = 4 - 3 \times (1) = 4 - (7 - 4) = 2 \cdot 4 - 7$

$= 2(60 - 7 \times 8) - 7 = 2 \cdot 60 - 17 \cdot 7$

or, $7 \cdot (-17) \equiv -1 \pmod{60}$,

∴ $K \equiv -17 \pmod{60}$ $\equiv 43 \pmod{60}$

$\therefore k = 17 + 60s$

From (VIII),

$x = 7 \times 17 + 7 \times 60s$

$= 119 + 420s$

$\therefore x \equiv 119 \pmod{420}$

$\therefore$ Least value of $x = 119$ (Ans.)

Alternate:

Notice, the least common multiple of the l.c.m. $(2, 3, 4, 5, 6) + 1$ will give remainders $(2-1), (3-1), (4-1), (5-1), (6-1)$ when divided by 2, 3, 4, 5, 6 respectively.

$\therefore x = k \times \text{lcm}(2, 3, 4, 5, 6) - 1$

$= 60k - 1$

And x is divisible by 7.

(9) Solve the eggs:

The basket of eggs problem is often phrased in the following form: One egg remains when the eggs are removed from the basket 2, 3, 4, 5, 6 at a time, but no eggs remains if they are removed 7 at a time. Find the smallest number of eggs that could have been in the basket.

$\Rightarrow$ $x \equiv 1 \pmod 2$
$x \equiv 1 \pmod 3$
$x \equiv 1 \pmod 4$
$x \equiv 1 \pmod 5$
$x \equiv 1 \pmod 6$

These are equivalent to:
$x \equiv 1 \pmod{\text{lcm}(2,3,4,5,6)}$
$\Rightarrow x \equiv 1 \pmod{60}$ ——— (i)

$x \equiv 0 \pmod 7$ ——— (ii)

Now, Using C.R.T,

$n = 7 \times 60 = 420$

$N_1 = 60, \; N_2 = 7$

∴ Inverse of N_1 modulo n_1 is:

$N_1 x \equiv 1 \pmod 7$

$\Rightarrow 60x \equiv 1 \pmod 7$

$\Rightarrow x_1 \equiv 2 \pmod 7$

and, inverse of N_2 modulo n_2 is:

$7x \equiv 1 \pmod{60}$

$\Rightarrow 7 \times (-17) \equiv 1 \pmod{60}$

$\therefore x_2 \equiv -17 \pmod{60}$

∴ Simultaneous sol^n of (i) and (ii) is:

$x \equiv N_1 x_1 b_1 + N_2 x_2 b_2 \pmod{420}$

$\equiv 60 \times 2 \times 6 + 7 \times (-17) \times 1 \pmod{420}$

$\equiv -119 \pmod{420}$

$\equiv 301 \pmod{420}$

∴ Smallest $x = 301$. (Ans)

(10) Ancient Chinese Problem:

A band of 17 pirates stole a sack of gold coins. When they tried to divide the fortune into equal portions, 3 coins remained. In the ensuing brawl over who should get the extra coins, one pirate was killed. The wealth was redistributed, but this time an equal division left 10 coins. Again an argument developed in which another pirate was killed. But now the total fortune was evenly distributed among the survivors.
What was the least number of coins, that could have been stolen?

⇒ Let, total number of coins = x

$\therefore x \equiv 3 \pmod{17}$
$x \equiv 10 \pmod{16}$
$x \equiv 0 \pmod{15}$

Now, 17, 16, 15 are pairwise coprimes.
$\therefore$ Unique soln exists.

Let, $n = 17 \times 16 \times 15$
$\therefore N_1 = 16 \times 15, \quad N_2 = 17 \times 15$

$\therefore N_1 x_1 \equiv 1 \pmod{n_1}$
or, $16 \times 15\, x_1 \equiv 1 \pmod{17}$
or, $-15\, x_1 \equiv 1 \pmod{17}$
or, $2 x_1 \equiv 1 \pmod{17}$
or, $x_1 \equiv 9 \pmod{17}$

$N_2 x_2 \equiv 1 \pmod{n_2}$
or, $17 \times 15\, x_2 \equiv 1 \pmod{16}$
or, $x_2 \equiv -1 \equiv 15 \pmod{16}$

$\therefore$ Simultaneous soln: $x \equiv 16 \times 15 \times 9 \times 3 + 17 \times 15 \times 15 \times 10 \pmod{n}$

or, $x \equiv 6,480 + 38,250 \pmod{4080}$
$\equiv 3930 \pmod{4080}$

$\therefore$ Smallest $x = 3930$. (Ans)

(11) Prove that the congruences:

$x \equiv c_1 \pmod{n_1}$

$x \equiv c_2 \pmod{n_2}$

admits a simultaneous sol^n, if and only if, $\gcd(n_1, n_2) \mid (c_1 - c_2)$

If a sol^n exists, confirm that it is unique modulo $\text{lcm}(n_1, n_2)$

⇒ (i) $x \equiv c_1 \pmod{n_1} \implies x = c_1 + n_1 t_1$

$x \equiv c_2 \pmod{n_2} \implies x = c_2 + n_2 t_2$

If x is the simultaneous (common) sol^n, then,

$c_1 + n_1 t_1 = c_2 + n_2 t_2$

or, $c_1 - c_2 = n_2 t_2 - n_1 t_1$

or, $c_1 - c_2 = vd\, t_2 - ud\, t_1$

or, $c_1 - c_2 = d(v t_2 - u t_1)$

$\therefore d \mid (c_1 - c_2)$

Let, $\gcd(n_1, n_2) = d$

$\therefore n_1 = ud$, $n_2 = vd$

where, u, v are coprime

Conversely,

Let, $\gcd(n_1, n_2) = d$

and, $d \mid (c_1 - c_2)$

$\therefore c_1 - c_2 = dk$

$= (n_1 s + n_2 t) k$ [$\because \exists s, t$ such that, $n_1 s + n_2 t = d$]

or, $c_1 - (sk) \cdot n_1 = c_2 + (tk) \cdot n_2$ ——— (i)

If, x_1 be the sol^n of $x \equiv c_1 \pmod{n_1}$, then, $x_1 \equiv c_1 \pmod{n_1}$

and, x_2 " " " $x \equiv c_2 \pmod{n_2}$, then, $x_2 \equiv c_2 \pmod{n_2}$

from (i),

$c_1 \equiv c_2 + (tk) n_2 \pmod{n_1}$

Let, $c_1 - (sk)\, n_1 = c_2 + (tk)\, n_2 = x_0$

$\therefore \quad x_0 \equiv c_1 \pmod{n_1}$

$x_0 \equiv c_2 \pmod{n_2}$

$\therefore$ x_0 is the simultaneous sol^n of $x \equiv c_1 \pmod{n_1}$ and, $x_0 \equiv c_2 \pmod{n_2}$

$\therefore \quad x \equiv c_1 \pmod{n_1}$ has a simultaneous sol^n, if and only if

$x \equiv c_2 \pmod{n_2}$

$\gcd(n_1, n_2) \mid (c_1 - c_2)$ (proved)

(ii) Let, y be any other sol^n of the system.

$\therefore \quad y \equiv c_1 \pmod{n_1}$

and, $y \equiv c_2 \pmod{n_2}$

$\therefore \quad x \equiv y \pmod{n_1}$
and, $x \equiv y \pmod{n_2}$ $\Longrightarrow$ $x \equiv y \pmod{\text{lcm}(n_1, n_2)}$

$\therefore$ x is unique sol^n module $\text{lcm}(n_1, n_2)$.

(12) Show that the following system does not possess a soln:

$x \equiv 5 \pmod 6$ and $x \equiv 7 \pmod{15}$

$\Rightarrow \gcd(6, 15) = 3 \nmid (7-5)$

$\therefore$ No soln exists.

---

(13) If, $x \equiv a \pmod n$, prove that either,

$x \equiv a \pmod{2n}$ or, $x \equiv a+n \pmod{2n}$

$\Rightarrow x \equiv a \pmod n$

$\Rightarrow x = a + Kn$

Now, K can be even or odd.

If K is even, then, $K = 2r$

$\therefore x = a + 2nr$

or, $x \equiv a \pmod{2n}$ ——— (i)

If K is odd, let, $K = 2r + 1$

$\therefore x = a + 2nr + n$

or $x \equiv a+n \pmod{2n}$ ——— (ii)

$\therefore$ Either $x \equiv a \pmod{2n}$, or, $x \equiv a+n \pmod{2n}$

(Proved)

---

(14) A certain integer between 1 and 1200 leaves the remainders 1, 2, 6 when divided by 9, 11, 13 respectively. What is the integer?

$\Rightarrow$ $x \equiv 1 \pmod 9$
$x \equiv 2 \pmod{11}$
$x \equiv 6 \pmod{13}$
} The integer is the simultaneous soln of this system.

$\because$ 9, 11, 13 are pairwise coprimes.
$\therefore$ Unique soln exist.

$n = 9 \times 11 \times 13$
$N_1 = 11 \times 13$
$N_2 = 9 \times 13$
$N_3 = 9 \times 11$

$\therefore$ By C.R.T, we get the integer:

$x \equiv 1 \times (11 \times 13) \times 8 + 2 \times (9 \times 13) \times 8 + 6 \times 9 \times 11 \times 5 \pmod{9 \times 11 \times 13}$

$9 \times 11 x \equiv 1 \pmod{13}$
$4 \times 2 x \equiv 1$
$\Rightarrow 8x \equiv 1$
$\Rightarrow x \equiv 5$

$11 \times 13 x \equiv 1 \pmod 9$
$2 \times 4 x \equiv 1$
$x \equiv -1 \equiv 8$

$9 \times 13 x \equiv 1 \pmod{11}$
$-2 \times 2 x \equiv 1$
$4x \equiv 1$
$x \equiv 3$

$\equiv 1,144 + 1,872 + 2,970 \pmod{1,287}$

$\equiv 838 \pmod{1,287}$

$\therefore$ The required number 838. (Ans)

---

(15) (a) Yih-hing:

Find an integer, having remainders 1, 2, 5, 5, when divided by 2, 3, 6, 12 respectively.

$\Rightarrow$ $x \equiv 1 \pmod 2$, or, $x \equiv -1 \pmod 2$ —— (2)
$x \equiv 2 \pmod 3$, or, $x \equiv -1 \pmod 3$ —— (3)
$x \equiv 5 \pmod 6$, or, $x \equiv -1 \pmod 6$ —— (6)
$x \equiv 5 \pmod{12}$, or, $x \equiv 5 \pmod{12}$ —— (12)

Simultaneous soln of (2), (3), (6) is,

$x \equiv -1 \pmod{\text{lcm}(2, 3, 6)}$

or, $x \equiv -1 \pmod 6$ —— (6)

or, $2x \equiv -2 \pmod{2 \times 6}$ [Multiplying by 2]

(1) $\Rightarrow 2x \equiv -2 \pmod{12}$ ——— (6')

(6') − (12) $\Rightarrow$

$2x - x \equiv -2 - 5 \pmod{12}$

$\Rightarrow x \equiv -7 \pmod{12}$

$\equiv 5 \pmod{12}$

$\equiv 17 \pmod{12}$ (Ans)

Bhaskara :-

(b) Find an integer having the remainders 2, 3, 4, 5, when divided by 3, 4, 5, 6 respectively.

$\Rightarrow$ $x \equiv 2 \pmod 3$, or, $x \equiv -1 \pmod 3$

$x \equiv 3 \pmod 4$, or, $x \equiv -1 \pmod 4$

$x \equiv 4 \pmod 5$, or, $x \equiv -1 \pmod 5$

$x \equiv 5 \pmod 6$, or, $x \equiv -1 \pmod 6$ } ——— (i)

$\therefore$ Simultaneous sol^n of (i) ns. system is;

$x \equiv -1 \pmod{\text{lcm}(3,4,5,6)}$

$\equiv -1 \pmod{60}$

$\equiv 59 \pmod{60}$ (Ans)

(c) Regiomontanus :

Find an integer having the remainders 3, 11, 15 when divided by 10, 13, 17 respectively.

$\Rightarrow$ $x \equiv 3 \pmod{10}$

$x \equiv 11 \pmod{13}$

$x \equiv 15 \pmod{17}$

$\because$ 10, 13, 17 are pairwise coprimes,

$\therefore$ Unique soln exists.

Let, $n = 10 \times 13 \times 17$

$N_1 = 13 \times 17$

$\therefore 13 \times 17\, x_1 \equiv 1 \pmod{10}$

or $x_1 \equiv 1 \pmod{10}$

$N_2 = 10 \times 17$

$\therefore 10 \times 17\, x_2 \equiv 1 \pmod{13}$

or $x_2 \equiv 1 \pmod{13}$

$N_3 = 10 \times 13$

$\therefore 10 \times 13\, x_3 \equiv 1 \pmod{17}$

or, $-7 \times -4\, x_3 \equiv 1$

or, $11\, x_3 \equiv 1$

or, $33\, x_3 \equiv 3$

or, $x_3 \equiv -3 \equiv 14$

$\therefore$ Simultaneous soln:

$$x \equiv 3 \times 13 \times 17 + 11 \times 10 \times 17 + 15 \times 10 \times 13 \times 14 \pmod{10 \times 13 \times 17}$$

$$\equiv 29,833 \pmod{2,210}$$

$$\equiv 1,103 \pmod{2,210}$$ (Ans)

---

(18) Obtain the two incongruent soln's modulo 210 of the system:

$2x \equiv 3 \pmod 5$ ——— (5)

$4x \equiv 2 \pmod 6$ ——— (6)

$3x \equiv 2 \pmod 7$ ——— (7)

$2x \equiv 3 \pmod 5$

or, $6x \equiv 9 \pmod 5$

or, $x \equiv 4 \pmod 5$ ——— (5)

and, $3x \equiv 2 \pmod 7$

or, $15x \equiv 10 \pmod 7$

or, $x \equiv 3 \pmod 7$ ——— (7)

Now, $4x \equiv 2 \pmod 6$ $\quad \because \gcd(4,6) = 2$

has two incongruent sol^{n}s.

$\Rightarrow$ or, $2x \equiv 1 \pmod 3$

or, $x \equiv 2 \pmod 3$

$\therefore$ Two incongruent sol^{n}s are:

$x \equiv 2, 2+3 \equiv 2, 5 \pmod 6$

$\therefore$ We have the modified system:

$x \equiv 4 \pmod 5$ ——— (5)

$x \equiv 2$ or, $5 \pmod 6$ ——— (6)

$x \equiv 3 \pmod 7$ ——— (7)

Now, 5, 6, 7 are pairwise coprimes.

$\therefore$ Let, $n = 5 \times 6 \times 7$, $N_1 = 6 \times 7$, $N_2 = 5 \times 7$, $N_3 = 5 \times 6$

$\therefore$ $6 \times 7\, x_1 \equiv 1 \pmod 5$ | $5 \times 7\, x_2 \equiv 1 \pmod 6$ | $30 x_3 \equiv 1 \pmod 7$

or, $x_1 \equiv 3 \pmod 5$ | or, $x_2 \equiv 5 \pmod 6$ | or, $x_3 \equiv 4 \pmod 7$

$\therefore$ By C.R.T we get, the simultaneous (two) sol^{n}s (incongruent)

$\therefore$ $\bar{x} \equiv 4 \times 3 \times 42 + 2 \times 5 \times 35 + 3 \times 4 \times 30 \pmod{210}$

$\equiv 1,214 \pmod{210}$

$\equiv 164 \pmod{210}$

or, $\bar{x} \equiv 4 \times 3 \times 42 + 5 \times 5 \times 35 + 3 \times 4 \times 30 \pmod{210}$

$\equiv 1,739 \pmod{210}$

$\equiv 59 \pmod{210}$

Ans

(17) Find the sol^n's of the system of congruences:

$3x + 4y \equiv 5 \pmod{13}$ ——— (i)

$2x + 5y \equiv 7 \pmod{13}$ ——— (ii)

⇒ Now, $\gcd(3\times5 - 4\times2, 13)$

$= \gcd(3, 13) = 1$

∴ This system has unique sol^n modulo 13.

(i) × 5 − (ii) × 4 ⇒ $7x \equiv -3 \equiv 10 \pmod{13}$

~~(ii) × 3 − (i) × 2 ⇒ 7x~~

or, $14x \equiv 20 \pmod{13}$

or, $x \equiv 7 \pmod{13}$

and, (ii) × 3 − (i) × 2 ⇒ $7y \equiv 11 \pmod{13}$

or, $14y \equiv 22 \pmod{13}$

or, $y \equiv 9 \pmod{13}$

∴ sol^n: $(x, y) \equiv (7, 9) \pmod{13}$ (Ans)

---

(20) (a) Solve the systems of congruences:

(a) $5x + 3y \equiv 1 \pmod{7}$ ——— (i)

$3x + 2y \equiv 4 \pmod{7}$ ——— (ii)

⇒ $\gcd(5\times2 - 3\times3, 7) = \gcd(1, 7) = 1$ ∴ Unique Sol^n exists

(i) × 2 − (ii) × 3 ⇒ $1.x \equiv 4 \pmod{7}$

(ii) × 5 − (i) × 3 ⇒ $y \equiv 3 \pmod{7}$ } (Ans)

(b) $7x + 3y \equiv 6 \pmod{11}$ ——— (i)

$4x + 2y \equiv 9 \pmod{11}$ ——— (ii)

$\Rightarrow \gcd(ad - bc, n) = \gcd(2, 11) = 1 \quad \therefore \exists$ unique soln.

(i) $\times 2$ — (ii) $\times 3 \Rightarrow 2x \equiv -15 \pmod{11}$

or, $2x \equiv 7 \pmod{11}$

or, $x \equiv 42 \equiv 9 \pmod{11}$

From (i), $3y \equiv 6 - 7 \times 9 \pmod{11}$

or, $12y \equiv 24 - 28 \times 9 \pmod{11}$

or, $y \equiv 2 + 1 \equiv 3 \pmod{11}$

$\therefore (x, y) \equiv (9, 3) \pmod{11}$ (Ans)

(c) $11x + 5y \equiv 7 \pmod{20}$ ——— (i)

$6x + 3y \equiv 8 \pmod{20}$ ——— (ii)

$\Rightarrow \gcd(ad - bc, n) = \gcd(3, 20) = 1$

$\therefore \exists$ unique soln.

(i) $\times 3$ — (ii) $\times 5 \Rightarrow 3x \equiv -19 \pmod{20}$

or, $x \equiv 7 \pmod{20}$ (Ans)

From (i); $5y \equiv 7 - 7 \times 11 \pmod{20}$

or, $5y \equiv 10 \pmod{20}$

$\gcd(5, 20) = 5 \mid 10$

$\therefore$ five incongruent soln's exist.

or, $y \equiv 2 \pmod{4}$

$\therefore y \equiv 2, 2+4, 2+8, 2+12 \pmod{20}$

$\equiv 2, 6, 10, 14 \pmod{20}$

$\therefore y \equiv 2, 7, 12, 17 \pmod{20}$ $\quad \therefore 3y \equiv 6 \pmod{20}$

$\therefore y \equiv 2, 6, 10, 14, 18 \pmod{20}$

But, (ii) is only satisfied by $y \equiv 2 \pmod{20}$

$\therefore$ So the only sol^n is : $x \equiv 7, y \equiv 2 \pmod{20}$

Caution :

So, it is advised to evaluate y, by eliminating x from both equations, not by putting value of x in one eq^n :~

(ii) $\times 11 -$ (i) $\times 6 \Rightarrow 3y \equiv 88 - 42 \pmod{20}$

or, $3y \equiv 6 \pmod{20}$

or, $y \equiv 2 \pmod{20}$ (Ans)

T

(19) Obtain the eight incongruent sol^{n}s of the linear congruence

$3x + 4y \equiv 5 \pmod{8}$

$\Rightarrow \gcd(3,4,8) = 1 \mid 5$

$\therefore$ This congruence has sol^{n}s.

Now, $3x \equiv 5 - 4y \pmod{8}$

Now, $\gcd(3,8) = 1 \mid (5 - 4y)$

So, there are 13 incongruent sol^{n}s of x for,

$y \equiv 0, 1, 2, \ldots 12 \pmod{13}$

for, $y \equiv 0$; $3x \equiv 5 \pmod{8}$, or, $x \equiv 7 \pmod{8}$

for, $y \equiv 1$; $3x \equiv 1$, or, $x \equiv 3 \pmod{8}$

for, $y \equiv 2$; $3x \equiv -3$, or, $x \equiv 7 \pmod{8}$

. . . . . .

in this way, we can evaluate all 13 incongruent sol^{n}s.

Alternate :~

$3x + 4y \equiv 5 \pmod 8$

Now, treating it as a Diophantine equation;

$\gcd(3,4) = 1 \mid 8$

$\therefore \quad 1 = 4(1) + 3(-1)$

or, $3(-5) + 4(5) \equiv 5 \pmod 8$

$\therefore \quad x_0 \equiv -5, \; y_0 \equiv 5 \pmod 8$ is a soln.

$\therefore$ General soln's :

$x \equiv -5 + 4t, \quad y \equiv 5 - 3t \pmod 8$

or, $x \equiv 3 + 4t, \quad y \equiv 5 - 3t \pmod 8$

~~Now for $t = 0, 1, 2, \ldots$~~

Now, t can have 8 incongruents values (modulo 8).

$\therefore$ Soln's are :

t	x	y
0	3	5
1	7	2
2	3	7
3	7	4
4	3	1
5	7	6
6	3	3
7	7	0
8	3	5
9		
10		
11		
12		

$\therefore$ Incongruent soln's are,

$(x, y) \equiv (3,5), (7,2), (3,7), (7,4), (3,1), (7,6), (3,3), (7,0) \pmod 8$

thus

(16) Let, t_n denote the nth triangular number.
For which value of n, does t_n divide $(t_1^2 + t_2^2 + \cdots + t_n^2)$

Hint: Because : $t_1^2 + t_2^2 + \cdots + t_n^2 = t_n \times \frac{3n^3 + 12n^2 + 13n + 2}{30}$

Obtain the values of n, for which,

$3n^3 + 12n^2 + 13n + 2 \equiv 0 \pmod{2 \times 3 \times 5}$

Important Note

(1) Suppose, for, $x \equiv 2 \pmod 9$ ——— (i)

if you multiply with an integer in both sides of the congruence where that integer is not coprime with 9, then, the number of soln's for (i) will change,

eg: $x \equiv 2 \pmod 9$ has unique soln

and, $3x \equiv 6 \pmod 9$ has $\gcd(3,9) = 3$ soln's ——— (ii)

So, be careful while multiplying with a number (c) in the both sides of the linear congruence, because extra soln's may be obtained, if c, and n are not coprime.

Here, (Soln set of (i)) $\subset$ (Soln set of (ii))

(i) → (ii) But, reverse not true. So (i) and (ii) are not equivalent

(2) $x \equiv 2 \pmod 9 \iff (x-2) = 9k$ for some k ——— (i)

or, $3(x-2) = 9 \times 3k$

or, $3x \equiv 3 \times 2 \pmod{9 \times 3}$

or, $3x \equiv 6 \pmod{27}$ ——— (ii)

Here, (i) has unique soln modulo 9,

and though (ii) has 3 incongruent soln's modulo 27, all the 3 incongruent soln's must satisfy (i).

So, (the soln set of (i)) = (the soln set of (ii))

You can do this type of multiplication (i.e, with changing the modulo also) for solving linear congruences.

(i) is equivalent to (ii), i.e, (i) $\leftrightarrow$ (ii)

FERMAT'S THEOREM

Fermat's Theorem :—

If p be a prime and $p \nmid a$, then, $a^{p-1} \equiv 1 \pmod{p}$

Proof :

Consider the first $(p-1)$ positive multiples of a, i.e,

$a, 2a, 3a, \ldots, (p-1)a$.

None of these are congruent modulo p to any other,

[Because, $1, 2, 3, \ldots, p-1$ are all incongruent to each other mod p]

nor, is any congruent to zero. [$\because a \not\equiv 0 \pmod{p}$ and, $1, 2, 3, \ldots, p-1 \not\equiv 0 \pmod{p}$]

Therefore the set of integers $\{a, 2a, 3a, \ldots, (p-1)a\}$ forms a residue class modulo p, i.e, this set must be congruent modulo p to $1, 2, 3, \ldots, p-1$, taken in some order.

Multiplying all these congruences together,

$a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \pmod{p}$

or, $a^{p-1} \cdot (p-1)! \equiv (p-1)! \pmod{p}$

or, $a^{p-1} \equiv 1 \pmod{p}$ [$\because \gcd(p, (p-1)!) = 1$]

(Proved)

FERMAT'S THEOREM

Corollary :

If p be a prime, then $\boxed{a^p \equiv a \pmod{p}}$ $\forall\ a \in \mathbb{N}$

Proof: **Case (i):** if $p \mid a$, then $a \equiv 0 \pmod{p}$

$\therefore a^p \equiv 0^p \equiv 0 \pmod{p}$

$\therefore a^p \equiv a \pmod{p}$

Case (ii): if $p \nmid a$, then by Fermat's th.,

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

$\Rightarrow a^p \equiv a \pmod{p}$ [multiplying by a]

$\therefore$ (Proved)

Proof by Induction :

To prove, $a^p \equiv a \pmod{p}$ where p is prime, $\forall\ a \in \mathbb{N}$,

we assume, $P(a) : a^p \equiv a \pmod{p}$ is true,

and we gotta prove $P(a+1)$ is true.

$\Rightarrow$ **Base Case:** for, $a = 0$, it holds, i.e, $P(0)$ is true.

Now, assuming $P(a)$ is true,

Now, $(a+1)^p = a^p + {}^pC_1 a^{p-1} + {}^pC_2 a^{p-2} + \cdots + {}^pC_{p-1} a + 1$

Now, ${}^pC_k = \dfrac{p!}{k! \cdot (p-k)!} \quad \forall \quad 1 \leq k \leq p-1$

or, $k! \times {}^pC_k = p(p-1)(p-2)\cdots(p-k+1) \equiv 0 \pmod p$

$\therefore p \mid (k! \times {}^pC_k)$

Now, $\because$ p is a prime,

$\therefore p \mid k!$ or, $p \mid {}^pC_k$

Now, $\because$ $1 \leq k \leq p-1$ and p is prime, $\therefore p \nmid k!$

$\therefore p \mid {}^pC_k$

$\therefore {}^pC_k \equiv 0 \pmod p$

$\therefore (a+1)^p \equiv a^p + 1 \pmod p$

$\equiv 1 \pmod p$ [assuming $P(a)$ is true]

$\therefore$ $P(a+1)$ is true, if $P(a)$ is true, and $P(0)$ is true.

$\therefore P(a)$ is true $\forall\ a \in \mathbb{N}$

(Proved)

Note :- It also happens, if a is a negative number, because, $a \equiv r \pmod p$ for some r, s.t, $0 \leq r \leq p-1$,

So, we get, $a^p \equiv r^p \equiv r \equiv a \pmod p$

Note

Applications of Fermat's Th. :~

(i) It can be labour saving for certain calculations:

Prove that, $5^{38} \equiv 4 \pmod{11}$

$\Rightarrow$ By Fermat's th.,

$5^{10} \equiv 1 \pmod{11}$

$\therefore 5^{38} \equiv (5^{10})^3 \cdot 5^8 \pmod{11}$

$\equiv 1 \times (25)^4 \equiv 3^4 \equiv 81 \equiv 4 \pmod{11}$

(ii) By Fermat's th., we can assure if a number is composite :~

If, $a^n \equiv a \pmod{n}$ fails to hold for some a, then, n is surely composite.

But if, it holds, we can't assure that n is prime

Eg: check for, $n = 117$

$\Rightarrow$ We assume $a = 2$,

$117 = 64 + 32 + 16 + 4 + 1$

$=$

$\therefore 2^{117} \equiv 2^{64} \cdot 2^{32} \cdot 2^{16} \cdot 2^4 \cdot 2$

$\equiv 44 \pmod{117}$

$\therefore$ 117 is composite.

Converse of Fermat's Th. is not necessarily true :-

Lemma :-

If p and q are distinct primes, with $a^p \equiv a \pmod q$ and, $a^q \equiv a \pmod p$, then, $a^{pq} \equiv a \pmod{pq}$

Proof :-

$$a^{pq} \equiv (a^p)^q \pmod q \qquad a^{pq} \equiv (a^q)^p \pmod p$$
$$\equiv a^q \pmod q \qquad \equiv a^p \pmod p$$
$$\equiv a \qquad \equiv a \pmod p$$

$\therefore q \mid (a^{pq} - a)$ and, $p \mid (a^{pq} - a)$

and, ~~q are distinct~~ p, q are coprimes.

$\therefore pq \mid a^{pq} - a$

$\Rightarrow a^{pq} \equiv a \pmod{pq}$

→ This is an example of the converse being false, $\because pq$ is composite.

Eg: $2^{340} \equiv 1 \pmod{341}$, but, $341 = 11 \times 31$

Pseudo Primes :~

If, n is composite, but, $2^n \equiv 2 \pmod{n}$, then n is called Pseudo Prime.

The smallest four Pseudo Primes to the base 2 are:

341; 561, 645, 1105.

(*) It can be shown that, there are infinitely many pseudo primes.

Theorem :

If n is an odd Pseudo Prime, then, $M_n = 2^n - 1$ is a larger pseudo prime

Proof:

(i) $\because$ n is composite, let, $n = rs$, where, $1 < r \leq s <$

$\therefore M_n = 2^n - 1 = 2^{rs} - 1 = (2^r - 1)(2^{r(s-1)} + 2^{r(s-2)} + \cdots t$

$\therefore$ M_n is composite.

(ii) $\because$ n is Pseudo Prime,

$\therefore 2^n \equiv 2 \pmod{n} \implies 2^n - 2 = kn$ for some k

Now, $2^{M_n - 1} - 1 = 2^{2^n - 2} - 1 = 2^{kn} - 1$

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

$\equiv 0 \pmod{2^n - 1}$

$\therefore 2^{M_n} \equiv 2 \pmod{M_n}$ and M_n is composite

$\therefore$ M_n is Pseudo Prime.

(*) In this way, we can construct an increasing seq of pseudoprimes.

More Generally:

A composite int n for which $a^n \equiv a \pmod{n}$ is true, is called a Pseudo Prime to the base a.

Absolute Pseudo Primes
or, Carmichael numbers:

There exist composite numbers, which are Pseudo primes, to every base a; ~~Integers a with gcd(a,n)~~ $= 1$.

These exceptional numbers are called absolute pseudo-primes or Charmichael numbers.

Eg: The least Charmichael no. is $561 = 3 \times 11 \times 17$

Note: ~~Supp~~ n is ~~Absolute Pseudo Prime~~, if n is square free, and canonical form of $n = p_1 p_2 \cdots p_k$

$(p_1 - 1)$

Note: Now, for the ints. a, for which $\gcd(a, 561) = 1$,

gives, $\gcd(a,3) = \gcd(a,11) = \gcd(a,17) = 1$

By Fermat's th., $a^2 \equiv 1 \pmod 3$ &

$a^{10} \equiv 1 \pmod{11}$

$a^{16} \equiv 1 \pmod{17}$

or, $\begin{cases} a^{560} \equiv (a^2)^{280} \equiv 1 \pmod{3} \\ a^{560} \equiv (a^{10})^{56} \equiv 1 \pmod{11} \\ a^{560} \equiv (a^{16})^{35} \equiv 1 \pmod{17} \end{cases}$

$\therefore a^{560} \equiv 1 \pmod{\text{lcm}(3, 11, 17)}$

or, $a^{560} \equiv 1 \pmod{561}$ $\forall$ a, s.t, $\gcd(a, 561) = 1$

or, $a^{561} \equiv a \pmod{561}$ $\forall\, a \in \mathbb{Z}$

$\therefore 561$ is Absolute Pseudo Prime.

Note: Absolute Pseudo Primes are Square free.

⇒ **Proof:** Suppose n is absolute pseudoprime.

$\therefore a^n \equiv a \pmod n \quad \forall\ a \in \mathbb{Z}$

Proof by contradiction:

If, n is not square-free, then let, $k^2 \mid n$ for some k.

then, if we let $a = k$,

then, $k^n \equiv k \pmod n \Rightarrow n \mid k^n - k$ and $k^2 \mid n$

$\because k^2 \mid n \quad \therefore k^n \equiv k \pmod{k^2}$

$\Rightarrow k^2 \mid k$, which is impossible,

that means, n must be square free.

Theorem: — (Converse may not be true)

Let n be a composite square free integer, say, $n = p_1 p_2 \cdots p_r$ where the p_i are distinct primes. If $(p_i - 1) \mid (n-1)\ \forall\ i = 1, 2, \ldots, r$ then, n is an absolute pseudo prime.

Proof: If, n is square-free, then the p_i are distinct primes.

Suppose, a is an integer satisfying $\gcd(a, n) = 1$,

$\therefore \gcd(a, p_i) = 1 \quad \forall\ i = 1(1)r$

By Fermat's th., $p_i \mid a^{p_i - 1} - 1$

and, from the given hypotheses, $(p_i - 1) \mid (n-1)$,

$n - 1 = k_i (p_i - 1)$ for some k_i

$\therefore a^{n-1} - 1 = a^{k_i (p_i - 1)} - 1$

$= (a^{p_i - 1} - 1)\{ a^{(p_i-1)(k-1)} + a^{(p_i-1)(k-2)} + \cdots + 1 \}$

$\therefore a^{p_i - 1} - 1 \mid a^{n-1} - 1$, and, $p_i \mid a^{p_i - 1} - 1$

$\Rightarrow p_i \mid a^{n-1} - 1 \quad \forall\ i = 1(1)r$

$\Rightarrow a^{n-1} \equiv 1 \pmod{p_i} \Rightarrow a^n \equiv a \pmod{p_i}$ $\forall\ a$ and $\forall\ i = 1(1)r$

$\Rightarrow a^n \equiv a \pmod{\text{lcm}(p_1, p_2, \ldots, p_r)} \Rightarrow a^n \equiv a \pmod n \ \forall\ a$

$\therefore n$ is absolute Pseudo Prime

Problems : 5.2

(1) Use Fermat's th. to verify that $17 \mid 11^{104} + 1$

$\Rightarrow$ By Fermat's th.,

$$11^{16} \equiv 1 \pmod{17} \quad [\because 17 \nmid 11]$$

$16 \mid 104$, 96, 8 | 6

Now, $11^{104} \equiv 11^{16 \times 6} \cdot 11^8 \pmod{17}$

$\equiv 1 \times 11^8 \pmod{17}$

$\equiv (-6)^8 \equiv 6^8 \equiv (36)^4 \equiv 2^4 \equiv 16$

$\equiv -1 \pmod{17}$

or, $11^{104} + 1 \equiv 0 \pmod{17}$

(2) (a) If $\gcd(a, 35) = 1$, show that $a^{12} \equiv 1 \pmod{35}$

$\Rightarrow \because \gcd(a, 35) = 1$

$\therefore \gcd(a, 5) = \gcd(a, 7) = 1 \quad [\because 35 = 5 \times 7]$

By Fermat's th., $a^4 \equiv 1 \pmod{5} \quad [\because 5 \nmid a]$ and, $a^6 \equiv 1 \pmod{7} \quad [\because 7 \nmid a]$

or, $(a^4)^3 \equiv 1^3 \pmod{5}$

or, $a^{12} \equiv 1 \pmod{5}$ — (i)

or, $a^{12} \equiv 1 \pmod{7}$ — (ii)

From (i) and (ii),

$a^{12} \equiv 1 \pmod{\text{lcm}(5, 7)}$

or, $a^{12} \equiv 1 \pmod{35}$ (Ans)

(b) If $\gcd(a, 42) = 1$, prove that $168 = 3.7.8$ divides $a^6 - 1$.

$\Rightarrow$ $\because \gcd(a, 42) = 1$ and, $42 = 2.3.7$

$\therefore \gcd(a, 2), \gcd(a, 3), \gcd(a, 7) = 1$

By Fermat's th.,

$a^1 \equiv 1 \pmod 2$

$\therefore a = 2k + 1$ for some k

$a^2 \equiv 1 \pmod 3$

or, $a^6 \equiv 1^3 \pmod 3$

or, $a^6 \equiv 1 \pmod 3$ (ii)

$a^6 \equiv 1 \pmod 7$ (iii)

$\therefore a^6 = (2k+1)^6$

$= \{8k^3 + 1 + 3.2k.1(2k+1)\}^2$

$= 64k^6 + 1 + \{6k(2k+1)\}^2 + 2.8k^3 + 2.6k(2k+1) + 2.6k(2k+1).8k^3$

$= 64k^6 + 1 + (12k + 6k)^2 + 2.8k^3 + 24k^2 + 12k + 2.6k.(2k+1).8k^3$

$\equiv 0 + 1 + (0 + 0 + 36k^2) + 0 + 0 + 4k + 0 \pmod 8$

$\therefore a^6 \equiv \{0 + 1 + 6k(2k+1)\}^2 \pmod 8$

$\equiv (1 + 12k^2 + 6k)^2 \pmod 8$

$\equiv (1 + 4k^2 + 6k)^2 \pmod 8$

$\equiv 1 + 16k^4 + 36k^2 + 8k^2 + 8.6k^3 + 12k \pmod 8$

$\equiv 1 + 0 + 4k^2 + 0 + 0 + 4k \pmod 8$

$\Rightarrow a^6 \equiv 1 + 4k(k+1) \pmod 8$

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

$\equiv 1 + 0$

$\equiv 1 \pmod 8$ ——— (i)

∵ we know that product of two consecutive ints. are divisible by 2
∴ $k(k+1) = 2m$

∴ from (i), (ii), (iii),

$a^6 \equiv 1 \pmod{\text{lcm}(3,7,8)}$

$\Rightarrow a^6 \equiv 1 \pmod{168}$ (Proved)

(c) If $\gcd(a,133) = \gcd(b,133) = 1$, show that,

$133 \mid a^{18} - b^{18}$

$\Rightarrow 133 = 7 \times 19$ ∴ $\gcd(a,19), \gcd(b,19) = 1$.

∴ Using Fermat's th.,

$a^{18} \equiv 1 \pmod{19}$ [$\because 19 \nmid a$] $b^{18} \equiv 1 \pmod{19}$ [$\because 19 \nmid b$]

∴ $a^{18} \equiv b^{18} \equiv 1 \pmod{19}$

$\Rightarrow a^{18} - b^{18} \equiv 0 \pmod{19}$ ——— (i)

Similarly, $a^6 \equiv b^6 \pmod 7$

$\Rightarrow (a^6)^3 \equiv (b^6)^3 \pmod 7$

$\Rightarrow a^{18} \equiv b^{18} \pmod 7$

$\Rightarrow a^{18} - b^{18} \equiv 0 \pmod 7$ ——— (ii)

From (i) and (ii); $a^{18} - b^{18} \equiv 0 \pmod{\text{lcm}(19,7)}$

$\Rightarrow a^{18} - b^{18} \equiv 0 \pmod{133}$ (Proved)

③ From Fermat's th., deduce that, for any integer $n \geq 0$,

$$13 \mid 11^{12n+6} + 1$$

$\Rightarrow$ By Fermat's th.,

$$11^{12} \equiv 1 \pmod{13}$$

$$\text{or, } (11^{12})^n \equiv 1^n \equiv 1$$

$$\text{or, } 11^{12n} \equiv 1$$

$$\therefore 11^{12n+6} + 1 \equiv (11)^{12n} \cdot 11^6 + 1$$

$$\equiv 1 \cdot (-2)^6 + 1 \pmod{13}$$

$$\equiv 64 + 1 \pmod{13}$$

$$\equiv 65 \pmod{13}$$

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

---

④ Derive each of the following congruences:

(a) $a^{21} \equiv a \pmod{15}$ $\forall a$.

$\Rightarrow$ By Fermat's th.,

$$a^5 \equiv a \pmod{5} \quad \text{and} \quad a^3 \equiv a \pmod{3}$$

$$\text{or, } a^{20} \equiv a^4 \pmod{5}$$

$$\text{or, } a^{21} \equiv a^5 \pmod{5}$$

$$\equiv a \pmod{5}$$

$$\text{or, } a^{21} \equiv (a^3)^7 \pmod{3}$$

$$\equiv a^7 \pmod{3}$$

$$\equiv (a^3)^2 \cdot a \pmod{3}$$

$$\equiv a^2 \cdot a \equiv a^3$$

$$\equiv a \pmod{3}$$

$$\therefore a^{21} \equiv a \pmod{\text{lcm}(3,5)}$$

$$\text{or, } a^{21} \equiv a \pmod{15}$$

(Proved)

(b) $a^7 \equiv a \pmod{42} \quad \forall a$

$\Rightarrow a^7 \equiv a \pmod 7$ | $a^3 \equiv a \pmod 3$ | $a^2 \equiv a \pmod 2$

$\therefore a^7 \equiv (a^3)^2 \cdot a \pmod 3$

$\equiv a^2 \cdot a \pmod 3$

$\equiv a^3 \pmod 3$

$\equiv a \pmod 3$

$\therefore a^7 \equiv (a^2)^3 \cdot a$

$\equiv a^3 \cdot a$

$\equiv (a^2)^2$

$\equiv a^2$

$\equiv a \pmod 2$

$\therefore a^7 \equiv a \pmod{\text{lcm}(2,3,7)}$

$\therefore a^7 \equiv a \pmod{42}$

(c) $a^{13} \equiv a \pmod{3.7.13} \quad \forall a$

$\Rightarrow a^3 \equiv a \pmod 3$ | $a^7 \equiv a \pmod 7$ | $a^{13} \equiv a \pmod{13}$

$\therefore a^{13} \equiv (a^3)^4 \cdot a$

$\equiv a^4 \cdot a$

$\equiv a^3 \cdot a^2$

$\equiv a \cdot a^2$

$\equiv a^3$

$\equiv a \pmod 3$

$\therefore a^{13} \equiv a^7 \cdot a^6$

$\equiv a \cdot a^6$

$\equiv a^7$

$\equiv a \pmod 7$

$\therefore a^{13} \equiv a \pmod{3.7.13}$

(d) Show that, $a^9 \equiv a \pmod{30} \quad \forall a$

$\Rightarrow 30 = 3 \times 5 \times 2$

$\therefore a^2 \equiv a \pmod 2$ | $a^3 \equiv a \pmod 3$ | $a^5 \equiv a \pmod 5$

$\therefore a^9 \equiv (a^2)^3 \cdot a$

$\equiv a^3 \cdot a$

$\equiv a^4$

$\equiv (a^2)^2 \equiv a^2$

$\equiv a \pmod 2$

$\therefore a^9 \equiv (a^3)^3$

$\equiv a^3$

$\equiv a \pmod 3$

$\therefore a^9 \equiv a^5 \cdot a^4$

$\equiv a \cdot a^4$

$\equiv a^5$

$\equiv a \pmod 5$

$\therefore a^9 \equiv a \pmod{\text{lcm}(2,3,5)}$

$\therefore a^9 \equiv a \pmod{30}$. (Proved)

(5) If, $\gcd(a, 30) = 1$, show that, $60 \mid a^4 + 59$

$\Rightarrow$ $30 = 2 \times 3 \times 5$

$\therefore \gcd(a, 2) = \gcd(a, 3) = \gcd(a, 5) = 1$

$\therefore a \equiv 1 \pmod 2$ | $a^2 \equiv 1 \pmod 3$ | $a^4 \equiv 1 \pmod 5$

or, $a = 2k + 1$ for some k | $\therefore a^4 \equiv (a^2)^2 \equiv 1^2 \equiv 1 \pmod 3$ | Qo

(iii) (iv)

$\therefore a^4 = (4k^2 + 4k + 1)^2$

$\equiv (0 + 0 + 1)^2 \pmod 4$

$\equiv 1 \pmod 4$ — (i)

From (i), (iv), (iii),

$a^4 \equiv 1 \pmod{\text{lcm}(4, 3, 5)}$

or, $a^4 \equiv 1 \pmod{60}$

or, $a^4 \equiv 1 - 60 \equiv -59$

$\therefore a^4 + 59 \equiv 0 \pmod{60}$ (Ans)

---

(6)(a) Find the units digit, of 3^{100} by the use of Fermat's th.

$3^{100} \pmod{10} = ?$

$\Rightarrow$ By Fermat's th.,

$3^2 \equiv 1 \pmod 2$ and, $3^4 \equiv 1 \pmod 5$

Alternative:

$3^2 \equiv 9 \equiv -1 \pmod{10}$

$\therefore 3^{100} \equiv (3^2)^{50} \equiv (-1)^{50} \equiv 1 \pmod{10}$ (Ans)

(6) For any integer a, verify that a^5 and a have the same units digit.

⇒ Say, $a \equiv r \pmod{10}$, [where, $0 \le r \le 9$]

Now, By Fermat's th.,

$a^2 \equiv a \pmod 2$ and, $a^5 \equiv a \pmod 5$

$\therefore a^5 \equiv a^2 \cdot a^2 \cdot a \pmod 2$

$\equiv a \cdot a \cdot a \pmod 2$

$\equiv a^2 \cdot a \pmod 2$

$\equiv a \cdot a \pmod 2$

$\equiv a^2 \equiv a \pmod 2$ —— (i)

From (i) and (ii); $a^5 \equiv a \pmod{\text{lcm}(2,5)}$

$\therefore a^5 \equiv a \pmod{10}$

$\equiv r \pmod{10}$

$\therefore$ Both a and a^5 have units digit r. (Proved)

---

(7) If, $7 \nmid a$, Prove that either a^3+1 or, a^3-1 is divisible by 7.

⇒ By Fermat's th.,

$a^6 \equiv 1 \pmod 7$

$\therefore, \quad a^6 - 1 \equiv 0 \pmod 7$

$\therefore, \quad (a^3+1)(a^3-1) \equiv 0 \pmod 7$

$\therefore \quad 7 \mid (a^3+1).(a^3-1)$

$\because$ 7 is prime, $\therefore$ 7 divides (a^3+1) or a^3-1

$\therefore \quad 7 \mid a^3+1$ or, $7 \mid a^3-1$

(8) The three most recent appearances of Halley's Comet were in the years 1835, 1910 and 1986, the next occurrence will be in 2061. Prove that,

$$1835^{1910} + 1986^{2061} \equiv 0 \pmod 7$$

$\Rightarrow 7 \nmid 1835$ and, $7 \nmid 1986$

$\therefore$ By Fermat's th.,

$1835^6 \equiv 1 \pmod 7$

$(1835)^{1910}$

$\equiv (1835^6)^{318} \cdot (1835)^2$

$\equiv 1 \cdot 1^2 \pmod 7$

$\equiv 1 \pmod 7$

$6)1910(318$
18
11
6
50
48
2

$7)1835(262$
14
43
42
15
14
1

$1986^6 \equiv 1 \pmod 7$

$\therefore (1986)^{2061}$

$\equiv (1986^6)^{343} \cdot (1986)^3$

$\equiv 1 \cdot 5^3 \pmod 7$

$\equiv 125 \pmod 7$

$\equiv -1 \pmod 7$

$6)2061(343$
18
26
24
21
18
3

$7)1986(283$
14
58
56
26
21
5

$\therefore 1835^{1910} + 1986^{2061} \equiv 1 - 1 \equiv 0 \pmod 7$ (Proved)

---

(9) (a) Let p be prime, $\gcd(a, p) = 1$. Use Fermat's th. to verify that $x \equiv a^{p-2} \cdot b \pmod p$ is a soln of the linear congruence $ax \equiv b \pmod p$

$\Rightarrow$ By Fermat's th., $a^{p-1} \equiv 1 \pmod p$ — (i)

Now, $ax \equiv b \pmod p$

or, $a \cdot a^{p-2} \cdot x \equiv b \cdot a^{p-2} \pmod p$

or, $a^{p-1} \cdot x \equiv b\, a^{p-2} \pmod p$

or, $1 \cdot x \equiv a^{p-2} \cdot b \pmod p$ [from (i)]

or, $x \equiv a^{p-2} \cdot b \pmod p$ (Proved)

(b) By applying part (a), solve the congruences $2x \equiv 1 \pmod{31}$, $6x \equiv 5 \pmod{11}$ and $3x \equiv 17 \pmod{29}$

$\Rightarrow$ (i) $2x \equiv 1 \pmod{31}$

$\therefore x \equiv 2^{31-2} \cdot 1 \pmod{31}$ [Assuming, $a = 2$, $b = 1$, $p = 31$]

$\equiv 2^{30} \equiv (32)^6 \pmod{31}$

$\equiv 1^6 \equiv \underline{1 \pmod{31}}$

(ii) $6x \equiv 5 \pmod{11}$

$\therefore x \equiv 6^{10} \cdot 5 \pmod{11}$

$\equiv 1.5 \pmod{11}$ [$\because$ Using Fermat's th., $6^{10} \equiv 1 \pmod{11}$]

$\equiv 5 \pmod{11}$

(iii) $3x \equiv 17 \pmod{29}$

$\therefore x \equiv 3^{29-1} \cdot 17 \pmod{29}$

$\equiv 17 \pmod{29}$ [$\because 3^{28} \equiv 1 \pmod{29}$]

(b) By applying part (a), solve the congruences
(i) $2x \equiv 1 \pmod{31}$, (ii) $6x \equiv 5 \pmod{11}$ (iii) $3x \equiv 17 \pmod{29}$

$\Rightarrow$ (i) $2x \equiv 1 \pmod{31}$

$\therefore x \equiv 2^{31-2} \cdot 1 \pmod{31}$ [Assuming, $a = 2$, $b = 1$, $p = 31$]

$\equiv 2^{29} \equiv (32)^5 \cdot 2^4 \pmod{31}$

$\equiv 1.16 \equiv \underline{16 \pmod{31}}$

(ii) $6x \equiv 5 \pmod{11}$

$\therefore x \equiv 6^{11-2} \cdot 5 \equiv 6^9 \cdot 5 \equiv 36^4 \cdot 6.5 \equiv 3^4 \cdot 30 \equiv 4.8$

$\equiv 32 \equiv \underline{10 \pmod{11}}$

(iii) $3x \equiv 17 \pmod{29}$

$\therefore x \equiv 3^{27} \cdot 17 \equiv (27)^9 \cdot 17 \equiv (-2)^9 \cdot 17$

$\equiv -1 \times 32 \times 16 \times 17 \equiv -1 \times 3 \times 16 \times -12$

$\equiv 36 \times 16 \equiv 7 \times 16 \equiv 112 \equiv 25 \pmod{29}$

---

(10) Assuming that a and b are ints, not divisible by the prime p, establish the following:

(i) if $a^p \equiv b^p \pmod{p}$, then $a \equiv b \pmod{p}$

(ii) If, $a^p \equiv b^p \pmod{p}$, then, $a^p \equiv b^p \pmod{p^2}$

⇒ (i) By Fermat's th.,

$a^p \equiv a \pmod{p}$ and, $b^p \equiv b \pmod{p}$

and, by the given hypothesis,

$a^p \equiv b^p \pmod{p}$

$\therefore a \equiv b \pmod{p}$ (proved)

(ii) By (i), we have $a \equiv b \pmod{p}$, if $a^p \equiv b^p \pmod{p}$

$\therefore a = b + pk$ for some k

$\therefore a^p - b^p = (b+pk)^p - b^p$

$= b^p + {}^pC_1 \cdot b^{p-1} \cdot pk + {}^pC_2 \cdot b^{p-2} \cdot p^2k^2 + \cdots$

$\cdots + {}^pC_{p-1} \cdot b \cdot (pk)^{p-1} + p^p k^p - b^p$

$= b^{p-1} \cdot p^2 \cdot k + {}^pC_2 \cdot b^{p-2} \cdot p^2k^2 + \cdots + p \times b \times p^{p-1} \cdot k^{p-1} + p^p \cdot k^p$

$\equiv 0 \pmod{p^2} \quad [\because p \geq 2]$

$\therefore a^p \equiv b^p \pmod{p^2}$ (Proved)

(11) Employ fermat's th., to prove that, if p is an odd prime, then,

(a) $1^{p-1} + 2^{p-1} + 3^{p-1} + \cdots + (p-1)^{p-1} \equiv -1 \pmod{p}$

(b) $1^p + 2^p + 3^p + \cdots + (p-1)^p \equiv 0 \pmod{p}$

⇒ (a) By fermat's th.,

$1^{p-1} \equiv 1 \pmod{p}$

$2^{p-1} \equiv 1 \pmod{p}$

$3^{p-1} \equiv 1 \pmod{p}$

$\vdots$

$(p-1)^{p-1} \equiv 1 \pmod{p}$

$\because$ p is prime.

$\therefore p \nmid i \quad \forall \quad 0 < i \leq p-1$

$1^{p-1} + 2^{p-1} + 3^{p-1} + \cdots + (p-1)^{p-1} \equiv \underbrace{1+1+1+\cdots+1}_{\leftarrow (p-1) \text{ terms} \rightarrow} \pmod{p}$

$\equiv p-1 \pmod{p}$

$\equiv -1 \pmod{p}$

(b) By fermat's th.,

$1^p + 2^p + 3^p + \cdots + (p-1)^p$

$\equiv 1 + 2 + 3 + \cdots + (p-1) \pmod{p}$

$\equiv \frac{p(p-1)}{2} \pmod{p}$

$\equiv p \times \left(\frac{p-1}{2}\right) \pmod{p}$

$\equiv 0 \times \left(\frac{p-1}{2}\right) \pmod{p}$

$\equiv 0 \pmod{p}$

$\because$ p is an odd prime $\therefore p-1 \geq 2$

$\therefore 2 \nmid p$

$\therefore$ 2 must divide $(p-1)$

$\therefore \frac{p-1}{2}$ is integer

(12) Prove that, if p is an odd prime and k is an integer satisfying, $1 \le k \le p-1$, then the binomial coeff.

$$ {}^{p-1}C_k \equiv (-1)^k \pmod{p} $$

$\Rightarrow$ $\because$ $1 \le k \le p-1$ and p is a prime.

By Fermat's th., $k^{p-1} \equiv 1 \pmod{p}$

Now, $${}^{p-1}C_k = \frac{(p-1)!}{k! \cdot (p-k-1)!}$$

or, $$k! \times {}^{p-1}C_k = (p-1)\cdot(p-2)\cdot(p-3)\cdots(p-k-k+1)$$
$$= (p-1)(p-2)(p-3)\cdots(p-k)$$
$$\equiv -1 \times -2 \times -3 \times \cdots \times -k \pmod{p}$$

or, $$k! \times {}^{p-1}C_k \equiv (-1)^k \cdot k! \pmod{p}$$

or, $${}^{p-1}C_k \equiv (-1)^k \pmod{p}$$

[$\because$ $0 \le k \le p-1$ and p is prime, $\therefore$ $\gcd(p, k!) = 1$]

(13) Assume that p and q are distinct odd primes such that, $p-1 \mid q-1$. If $\gcd(a, pq) = 1$, show that, $a^{q-1} \equiv 1 \pmod{pq}$

$\Rightarrow$ $\because \gcd(a, pq) = 1$

$\therefore \gcd(a, p) ; \gcd(a, q) = 1$

$\therefore p \nmid a$ and $q \nmid a$

By Fermat's th.,

$a^{p-1} \equiv 1 \pmod{p}$ | $a^{q-1} \equiv 1 \pmod{q}$ ——— (ii)

Again, by the given hypothesis,

$p-1 \mid q-1$. Let, $q-1 = k(p-1)$

$\therefore a^{p-1} \equiv 1 \pmod{p}$

$\Rightarrow a^{k(p-1)} \equiv 1^k \pmod{p}$

$\Rightarrow a^{q-1} \equiv 1 \pmod{p}$ ——— (i)

From (i) and (ii),

$a^{q-1} \equiv 1 \pmod{\text{lcm}(p, q)}$

$\Rightarrow a^{q-1} \equiv 1 \pmod{pq}$ (Proved)

(14) If, p and q are distinct primes, prove that,

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$$

⇒ ∵ p and q are distinct primes. ∴ $p \nmid q$ and $q \nmid p$.

By Fermat's Th.,

$$p^{q-1} \equiv 1 \pmod{q} \quad \text{and,} \quad q^{p-1} \equiv 1 \pmod{p}$$

~~$\therefore p^{q-1} = 1 + qs$ for some s~~ | ~~$\therefore q^{p-1} = 1 + pk$ for some~~

and, $q^{p-1} \equiv 0 \pmod{q}$ obviously | and, $p^{q-1} \equiv 0 \pmod{p}$ obviously

$\therefore p^{q-1} + q^{p-1} \equiv 1 \pmod{q}$ — (i) | $\therefore p^{q-1} + p^{p-1} \equiv 1 \pmod{p}$ — (ii)

from (i) and (ii),

$$p^{q-1} + q^{p-1} \equiv 1 \pmod{\text{lcm}(p,q)}$$

or, $p^{q-1} + q^{p-1} \equiv 1 \pmod{pq}$ [$\because \gcd(p,q) = 1$]

---

(15) Establish the statements below;

(a) If the number $M_p = 2^p - 1$ is composite, where p is a prime, then M_p is a pseudo prime.

⇒

(22) Establish the congruence:

$$2222^{5555} + 5555^{2222} \equiv 0 \pmod 7$$

⇒ Now, $1111 \equiv 5 \pmod 7$

By Fermat's th.,

~~$1111^6 \equiv 1 \pmod 7$~~ and, $2^6 \equiv 1 \pmod 7$

and, $5^6 \equiv 1 \pmod 7$

$\therefore 2222^{5555} \equiv (2 \times 1111)^{5555}$

$\equiv 2^{5555} \times 5^{5555}$

$\equiv (2^6)^{925} \cdot 2^5 \times 1$

$\equiv (2 \times 5)^{5555} \pmod 7$

$\equiv (2 \times 5)^{6 \times 925} \cdot (2 \times 5)^5 \pmod 7$

$\equiv (2^6 \times 5^6)^{925} \times 3^5 \pmod 7$

$\equiv 1 \times -2 \pmod 7$

and, $5555^{2222} \equiv (5 \times 1111)^{2222} \pmod 7$

$\equiv (5 \times 5)^{2222} \pmod 7$

$\equiv 5^{4444} \pmod 7$

$\equiv (5^6)^{740} \cdot 5^4 \pmod 7$

$\equiv 1 \cdot 16 \pmod 7$

$\equiv 2 \pmod 7$

$\therefore 2222^{5555} + 5555^{2222} \equiv -2 + 2 \equiv 0 \pmod 7$

(15) Establish the statements:

(a) If the number, $M_p = 2^p - 1$ is composite, where p is a prime, then, M_p is a Pseudo Prime.

$\Rightarrow$ $\because p$ is prime,
By Fermat's th., $2^p \equiv 2 \pmod{p}$

$\therefore 2^p - 2 = kp$ ——— (i)

Now, $2^{M_p - 1} - 1 = 2^{2^p - 2} - 1$

$= 2^{kp} - 1$

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

$\equiv 0 \pmod{2^p - 1}$

or, $2^{M_p - 1} \equiv 1 \pmod{M_p}$

$\therefore 2^{M_p} \equiv 2 \pmod{M_p}$

$\therefore M_p$ is a Pseudo Prime. (Proved)

(b) Every composite number $F_n = 2^{2^n} + 1$ is a Pseudo Prime ($n = 0, 1, 2, \ldots$)

$\Rightarrow$ We gotta proove, $2^{F_n} \equiv 2 \pmod{F_n}$.

or, $2^{2^{2^n}+1} \equiv 2 \pmod{2^{2^n}+1}$

Now, $2^{n+1} \mid 2^{2^n}$ $\quad [\because n+1 \leq 2^n \ \forall\ n \geq 0]$

$\therefore 2^{2^n} + 1$

$\Rightarrow 2^{2^{n+1}} - 1 \mid 2^{2^n} - 1$ ——— (i)

Again, $2^{2^{n+1}} - 1 = 2^{2^n \cdot 2} - 1 = (2^{2^n})^2 - 1$

$= (2^{2^n} + 1)(2^{2^n} - 1)$

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

$\therefore f_n \mid 2^{2^{n+1}} - 1$ ——— (ii)

From (i) and (ii); $f_n \mid 2^{2^{n+1}} - 1$

or, $2^{2^{2^n}} \equiv 1 \pmod{f_n}$

or, $2^{2^{2^n}+1} \equiv 2 \pmod{f_n}$

or, $2^{f_n} \equiv 2 \pmod{f_n}$

$\therefore f_n$ is absolute pseudo prime.

(16) Confirm the following integers are absolute pseudo prime

(a) $1105 = 5 \cdot 13 \cdot 17$

(b) $2821 = 7 \cdot 13 \cdot 31$

(c) $2465 = 5 \cdot 17 \cdot 29$

$\Rightarrow$ (a) $1105 = 5 \cdot 13 \cdot 17$ is a square free composite

Now, $5-1 = 4 \mid 1104$ [$1105 - 1 = 1104$]

$13-1 = 12 \mid 1104$

$17-1 = 16 \mid 1104$

$\therefore$ 1105 is not absolute pseudo prime.

(a) Let, a is an int, s.t, $\gcd(a, 1105) = 1$.

$\therefore \gcd(a,5) = \gcd(a,13) = \gcd(a,17) =$

$\therefore a^4 \equiv 1 \pmod 5$, $\therefore a^{1104} \equiv (a^4)^{276}$

$a^{12} \equiv 1 \pmod{13}$ $\equiv 1 \pmod 5$

$a^{16} \equiv 1 \pmod{17}$ $\therefore a^{1104} \equiv (a^{12})^{92} \equiv 1 \pmod{13}$

$\therefore a^{1104} \equiv (a^{16})^{69} \equiv 1 \pmod{13}$

$\therefore a^{1104} \equiv 1 \pmod{\text{lcm}(5,13,17)}$

or, $a^{1105} \equiv a \pmod{1105}$

$\therefore$ 1105 is an absolute pseudo prime

(17) Show that, pseudoprime 341 is not an absolute pseudo prime, by showing that $\because 11^{341} \not\equiv 11 \pmod{341}$

$\Rightarrow 341 = 11 \times 31$

Now, $\because$ 11 and 31 are primes.

$11^{10} \equiv 1 \pmod{11}$

$\therefore 11^{340} \equiv (11^{10})^{34} \equiv 1 \pmod{11}$

$\rightsquigarrow 11^{341} \equiv 11 \pmod{11}$

$11^{30} \equiv 1 \pmod{31}$

$\therefore 11^{340} \equiv (11^{30})^{11} \cdot 11^{10} \pmod{31}$

$\equiv 1 \cdot 11^{10} \pmod{31}$

$\equiv (121)^5 \pmod{31}$

$\equiv (-3)^5 \pmod{31}$

$\equiv -27 \times 9 \pmod{31}$

$\equiv 30 \times 4 \times 9 \pmod{31}$

$\equiv 22 \pmod{31}$

$\therefore 11^{341} \not\equiv 11 \pmod{31}$

$\therefore 11^{341} \not\equiv 11 \pmod{11 \times 31}$

$\therefore$ 341 is not absolutely pseudo prime.

Alternative :—

$341 = 11 \times 31$

Now, $11 - 1 = 10 \mid 340$

But, $31 - 1 = 30 \nmid 340$

$\therefore$ 341 is not absolute pseudoprime.