STUDY MATERIALS
ON
Congruence Relation
Subject : Mathematics
Paper : GE2T.
Unit – 2.

Dr. Sangita chakraborty
Associate Professor
Deptt. of Mathematics
Kharagpur College.
Any query at Whatsup No: 9434455417.

NUMBER SYSTEM [Congruence Relation between Integers]

CONGRUENCE → Karl Friedrich Gauss, a German Mathematician introduced this concept which laid the foundation of modern theory of numbers.

Definition → Let m be a fixed positive integer. Two integers a and b are said to be congruent modulo m if $a-b$ is divisible by m.
It is denoted by $a \equiv b \pmod{m}$.

<u>eg</u>. Let $m = 5$; $1 \equiv 6 \pmod 5$, $-4 \equiv 11 \pmod 5$, $10 \equiv 0 \pmod 5$

If $a-b$ is not divisible by m, $a \not\equiv b \pmod m$, then a is said to be incongruent to b modulo m.

<u>eg</u>. $2 \not\equiv 6 \pmod 5$.

<u>Note</u>: when $m = 1$, every two integers are congruent modulo m. So usually m is taken to be a positive integer > 1.

Properties → [Proofs of these properties are given later]

1. $a \equiv a \pmod m$ → reflexive
2. If $a \equiv b \pmod m$, then $b \equiv a \pmod m$ → symmetric.
3. If $a \equiv b \pmod m$, and $b \equiv c \pmod m$, then $a \equiv c \pmod m$ → transitive
4. If $a \equiv b \pmod m$, then for any $c \in \mathbb{Z}$,
$$a + c \equiv (b+c) \pmod m$$
$$a \cdot c \equiv b \cdot c \pmod m$$
5. If $a \equiv b \pmod m$, and $c \equiv d \pmod m$, then
$$a \pm c \equiv (b \pm d) \pmod m$$
$$a \cdot c \equiv b \cdot d \pmod m$$
6. If $a \equiv b \pmod m$ and $d \mid m$, $d > 0$, then $a \equiv b \pmod d$

Definition → If $a \equiv b \pmod m$ then b is said to be a <u>residue of a modulo m</u>.

By Division ~~a~~ algorithm $\exists\, q \in \mathbb{Z}, r \in \mathbb{Z}$ s.t.
$$a = q \cdot m + r, \quad 0 \le r < m.$$
Since $a - r = q \cdot m \Rightarrow a \equiv r \pmod m$
$\Rightarrow r$ is a residue of a modulo m.

r is said to be the <u>least non-negative residue of a modulo m</u>.

The whole set $\mathbb{Z}$ of integers is divided into only m distinct and disjoint subsets, called the <u>residue classes modulo m</u>, denoted by

$$\bar{0} = \{0, \pm m, \pm 2m, \cdots\} = \{mk : k \in \mathbb{Z}\}$$
$$\bar{1} = \{1, 1 \pm m, 1 \pm 2m, \cdots\} = \{mk+1 : k \in \mathbb{Z}\}$$
$$\vdots$$
$$\{mk + (m-1) : k \in \mathbb{Z}\} = \overline{m-1} = \{m-1, (m-1) \pm m, (m-1) \pm 2m, \cdots\}$$

[Any two integers in a residue class are congruent modulo m whereas they are not when belonging to different residue cla[sses]]

Theorem: For any $a \in \mathbb{Z}, b \in \mathbb{Z}$, $a \equiv b \pmod m$ if and only if a and b leaves the same remainder when divided by m.

Proof: Let r be the remainder when a is divided by m. Then $\exists$ some $q \in \mathbb{Z}$ s.t. $a = q \cdot m + r$, $0 \le r < m$.

Since $a \equiv b \pmod m$, $a - b = K \cdot m$, $K \in \mathbb{Z}$.

$\Rightarrow b = a - K \cdot m = (q - K) \cdot m + r$

$\Rightarrow$ b leaves the same remainder r, when divided by m.

Conversely, let r be the same remainder when a and b are divided by m. Then $\exists$ some $q_1, q_2 \in \mathbb{Z}$ s.t. $a = q_1 m + r$, $b = q_2 \cdot m + r$

$\Rightarrow a - b = (q_1 - q_2) \cdot m \Rightarrow m \mid a - b \Rightarrow a \equiv b \pmod m$.

eg. $34 \equiv 4 \pmod 6$; $34 = 5 \cdot 6 + 4$, $4 = 0 \cdot 6 + 4$

Theorem: If $a \equiv b \pmod m$ then $a^n \equiv b^n \pmod m$, $\forall n \in \mathbb{Z}^+$.

We use the principle of Mathematical Induction to prove the theorem.

The Theorem is true for $n = 1$.

Let us assume that the theorem is true for some $K \in \mathbb{Z}^+$. Then $a^K \equiv b^K \pmod m$.

Now $a^K \equiv b^K \pmod m$ and $a \equiv b \pmod m$ together

$\Rightarrow a^K \cdot a \equiv b^K \cdot b \pmod m$

$\Rightarrow a^{K+1} \equiv b^{K+1} \pmod m$.

$\therefore$ The theorem is true for the positive integer $K+1$ if we assume it to be true for $K \in \mathbb{Z}^+$.

$\therefore$ By the principle of Induction,

$$a^n \equiv b^n \pmod m, \ \forall n \in \mathbb{Z}^+.$$

Alternatively, $a^K \equiv b^K \pmod m \Rightarrow a^K - b^K = q_1 m$, $q_1 \in \mathbb{Z}$.

$a \equiv b \pmod m \Rightarrow a - b = q_2 \cdot m$, $q_2 \in \mathbb{Z}$.

Now, $a \cdot (a^K - b^K) = (a \cdot q_1) \cdot m$, and $b^K \cdot (a - b) = (b^K q_2) \cdot m$

$\Rightarrow a \cdot (a^K - b^K) + b^K \cdot (a - b) = (a q_1 + b^K q_2) \cdot m$

$\Rightarrow a^{K+1} - \cancel{a b^K} + \cancel{a b^K} - b^{K+1} = (a q_1 + b^K q_2) \cdot m$

$\Rightarrow a^{K+1} - b^{K+1} = (a q_1 + b^K q_2) \cdot m$

$\Rightarrow a^{K+1} \equiv b^{K+1} \pmod m$

The Converse is NOT True:-

example, $3^2 \equiv 5^2 \pmod 4$ but $3 \not\equiv 5 \pmod 4$

$5^3 \equiv 8^3 \pmod 9$ but $5 \not\equiv 8 \pmod 9$.

Proof of the properties of Congruence Relation :-

① $a \equiv a \pmod m$ → reflexive property

<u>Proof:</u> $a-a$ is divisible by m, where m be a fixed +ve integer.

i.e., $a \equiv a \pmod m$.

② If $a \equiv b \pmod m$, then $b \equiv a \pmod m$ → Symmetric prop.

<u>Proof:</u> $a \equiv b \pmod m \Rightarrow a-b$ is divisible by m.
$\Rightarrow b-a$ " " " m.
$\Rightarrow b \equiv a \pmod m$.

③ If $a \equiv b \pmod m$ and $b \equiv c \pmod m$, then $a \equiv c \pmod m$.
This is transitive prop.

<u>Proof:</u> $a \equiv b \pmod m$ & $b \equiv c \pmod m$
$\Rightarrow m \mid (a-b)$ & $m \mid (b-c)$
$\Rightarrow a-b = k_1 m$ & $b-c = k_2 m$; $k_1, k_2 \in \mathbb{Z}$.
Now $a-c = (a-b)+(b-c) = (k_1+k_2)\cdot m$; $k_1+k_2 \in \mathbb{Z}$.
$\Rightarrow m \mid a-c \Rightarrow a \equiv c \pmod m$.

<u>Remarks:</u>
Therefore, from ①, ② & ③, it is understood that Congruence relation is an equivalence relation.

④ If $a \equiv b \pmod m$, then for any/all $c \in \mathbb{Z}$,
(i) $a+c \equiv (b+c) \pmod m$; (ii) $a\cdot c \equiv b\cdot c \pmod m$.

<u>Proof:</u> (i) $a \equiv b \pmod m \Rightarrow m \mid (a-b) \Rightarrow a-b = k\cdot m$; $k \in \mathbb{Z}$.
Now, $(a+c)-(b+c) = a-b = k\cdot m$
$\therefore$ $a+c \equiv (b+c) \pmod m$.
(ii) $a\cdot c - b\cdot c = (a-b)\cdot c = k m \cdot c = (kc)\cdot m$; $kc \in \mathbb{Z}$.
$\Rightarrow a\cdot c \equiv b\cdot c \pmod m$.

⑤ If $a \equiv b \pmod m$, and $c \equiv d \pmod m$, then
(i) $a \pm c \equiv (b \pm d) \pmod m$; (ii) $a\cdot c \equiv b\cdot d \pmod m$

<u>Proof:</u> (i) $a \equiv b \pmod m \Rightarrow m \mid (a-b) \Rightarrow a-b = k_1 m$, $k_1 \in$
$c \equiv d \pmod m \Rightarrow m \mid (c-d) \Rightarrow c-d = k_2 m$, $k_2 \in$
Now $a \pm c = (b+k_1 m) \pm (d+k_2 m) = (b \pm d) + (k_1 \pm k_2)\cdot m$
$\Rightarrow (a \pm c) - (b \pm d) = (k_1 \pm k_2)\cdot m \Rightarrow a \pm c \equiv (b \pm d) \pmod m$
(ii) $a\cdot c = (b+k_1 m)\cdot(d+k_2 m) = bd + (bk_2 + dk_1 + k_1 k_2 m)\cdot m$
$\Rightarrow a\cdot c - b\cdot d = (bk_2 + dk_1 + k_1 k_2 m)\cdot m \Rightarrow a\cdot c \equiv b\cdot d \pmod m$.

(6) If $a \equiv b \pmod{m}$ and $d|m$, $d>0$, then
$a \equiv b \pmod{d}$.

Proof: $a \equiv b \pmod{m} \Rightarrow m|(a-b) \Rightarrow a-b = Km; K \in \mathbb{Z}$.
And $d|m \Rightarrow m = r.d$; $r \in \mathbb{Z}$.
$\therefore$ $a-b = Km = K(r.d) = (Kr).d$; $Kr \in \mathbb{Z}$.
$\Rightarrow d|(a-b) \Rightarrow \underline{a \equiv b \pmod{d}}$.

Ex: Prove that if f be a polynomial with integral coefficients and if $f(a) \equiv K \pmod{m}$, then
$f(a+m) \equiv K \pmod{m}$.

Let $f(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_n x^n$; $c_i \in \mathbb{Z}, \forall i$
$f(a) = c_0 + c_1 a + c_2 a^2 + \cdots + c_n a^n$
& $f(a+m) = c_0 + c_1(a+m) + \cdots + c_n(a+m)^n$.
$= (c_0 + c_1 a + c_2 a^2 + \cdots + c_n a^n) + m.q$; $q \in \mathbb{Z}$.
$\therefore$ $f(a+m) = f(a) + m.q \equiv f(a) \pmod{m} + 0 \pmod{m}$,
$\Rightarrow f(a+m) \equiv f(a) \pmod{m}$, since $m.q \equiv 0 \pmod{m}$.
$\therefore$ $\underline{f(a+m) \equiv K \pmod{m}}$. , since $f(a) \equiv K \pmod{m}$.

Ex: Use the theory of congruences to prove:

(i) $7 \mid (2^{5n+3} + 5^{2n+3})$; $\forall n \geq 1, n \in \mathbb{Z}$.

(ii) $43 \mid (6^{n+2} + 7^{2n+1})$; $\forall n \geq 1, n \in \mathbb{Z}$.

(iii) $17 \mid (2^{3n+1} + 3.5^{2n+1})$; $\forall n \geq 1, n \in \mathbb{Z}$.

Solution:

(i) $2^{5n+3} + 5^{2n+3} = 2^3.(2^5)^n + 5^3.(5^2)^n = 8.32^n + 125.25^n$.

Now, $32 \equiv 25 \pmod 7$

$\Rightarrow 32^n \equiv 25^n \pmod 7$, $\forall n \geq 1$. [using the fact; $a \equiv b \pmod m \Rightarrow a^n \equiv b^n \pmod m$]

or, $8.32^n \equiv 8.25^n \pmod 7$, by property ④.

$\Rightarrow 8.32^n - 8.25^n \equiv 0 \pmod 7 \longrightarrow ①$

Also we have, $133.25^n \equiv 0 \pmod 7 \longrightarrow ②$

$\therefore$ From ① & ②, we get

$8.32^n - 8.25^n + 133.25^n \equiv 0 \pmod 7$, by prop ⑤ :-

a, $8.32^n + 125.25^n \equiv 0 \pmod 7$

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

(ii) $6^{n+2} + 7^{2n+1} = 6^2.6^n + 7.(7^2)^n = 36.6^n + 7.49^n$.

Now $6 \equiv 49 \pmod{43}$

$\Rightarrow 6^n \equiv 49^n \pmod{43}$, $\forall n \geq 1$

$\Rightarrow 36.6^n - 36.49^n \equiv 0 \pmod{43} \longrightarrow ①$.

Also, $43.49^n \equiv 0 \pmod{43} \longrightarrow ②$.

From ① & ②, we get

$36.6^n - 36.49^n + 43.49^n \equiv 0 \pmod{43}$

a, $6^2.6^n + 7.49^n \equiv 0 \pmod{43}$

$\Rightarrow 43 \mid (6^{n+2} + 7^{2n+1})$, $\forall n \geq 1$.

(iii) $2^{3n+1} + 3.5^{2n+1} = 2.8^n + 3.5.25^n$

Now $8 \equiv 25 \pmod{17}$

$\Rightarrow 8^n \equiv 25^n \pmod{17}, \ \forall n \geqslant 1.$

or, $2.8^n - 2.25^n \equiv 0 \pmod{17} \longrightarrow (1).$

Also, $17.25^n \equiv 0 \pmod{17} \longrightarrow (2).$

From (1) & (2), we get

$$2.8^n - 2.25^n + 17.25^n \equiv (0+0) \pmod{17}$$

or, $2.8^n + 15.25^n \equiv 0 \pmod{17}$

i.e., $17 \mid (2^{3n+1} + 3.5^{2n+1})$.

Ex: Prove that $1! + 2! + \cdots + 1000! \equiv 3 \pmod{15}$.

Now, $(5+n)! \equiv 0 \pmod{15}$ for $n \geqslant 0, n \in \mathbb{Z}$.

Again, $1! + 2! + 3! + 4! = 33 \equiv 3 \pmod{15}$

$\therefore \ (1! + 2! + 3! + 4!) + (5! + 6! + \cdots + 1000!)$

$\equiv 3 \pmod{15} + 0 \pmod{15}$

$\equiv 3 \pmod{15}$. (proved)

Ex: Find the remainder when $1! + 2! + 3! + \cdots + 100!$ is divided by 24.

$4! \equiv 0 \pmod{24}$, and for any +ve integer n,

$(4+n)! \equiv 0 \pmod{24}$.

Therefore, $1! + 2! + 3! + 4! + \cdots + 100!$

$\equiv (1! + 2! + 3!) \pmod{24}$

$\equiv 9 \pmod{24}$.

$\therefore$ The remainder is $\underline{9}$.

Theorem: If $a.x \equiv a.y \pmod m$ and $\gcd(a,m)=1$, then $x \equiv y \pmod m$

Proof: $ax - ay = q.m$, $q \in \mathbb{Z}$.

$\Rightarrow x - y = \frac{q.m}{a}$. Since $x-y$ is an integer, $\therefore a \mid q.m$.

Since $\gcd(a,m)=1$, $\therefore a \mid q \Rightarrow q = K.a$, $K \in \mathbb{Z}$.

$\therefore x - y = \frac{K.a.m}{a} = K.m \Rightarrow x \equiv y \pmod m$.

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

We have $ax - ay = q.m$, $q \in \mathbb{Z}$.

Since $\gcd(a,m) = d$, $a = d.r$, $m = d.s$; $r, s \in \mathbb{Z}$, and prime to each other

$\therefore d.r.x - d.r.y = q.d.s$

$\Rightarrow r.(x-y) = q.s \Rightarrow x - y = \frac{q.s}{r}$

Since $x-y$ is an integer, $r \mid q.s \Rightarrow r \mid q$, since $\gcd(r,s) = 1$.

i.e., $\frac{q}{r}$ is an integer, say, K.

$\therefore x - y = K.s = K.\left(\frac{m}{d}\right) \Rightarrow x \equiv y \pmod{\frac{m}{d}}$.

Conversely. Let $x \equiv y \pmod{\frac{m}{d}}$. $\Rightarrow \frac{m}{d} \mid (x-y)$

$\Rightarrow m \mid d(x-y) \Rightarrow m \mid a(x-y)$

$\Rightarrow ax \equiv ay \pmod m$.

Corollary: If $ax = ay \pmod m$ and $a \mid m$ then $x \equiv y \pmod{\frac{m}{a}}$.

$ax - ay = q.m$, for $q \in \mathbb{Z}$.

$x - y = \frac{qm}{a} = K.q$ [where $\frac{m}{a} = K \in \mathbb{Z}$, since $a \mid m$]

$\therefore x \equiv y \pmod K \Rightarrow x \equiv y \pmod{\frac{m}{a}}$.

Theorem: $x \equiv y \pmod{m_i}$, for $i = 1, 2, \cdots, r$
$\Leftrightarrow x \equiv y \pmod m$, where $m = [m_1, m_2, \cdots, m_r]$, the l.c.m. of m_i's. $i = 1, 2, \cdots, r$.

$x \equiv y \pmod{m_i} \Rightarrow m_i \mid (x-y)$, for $i = 1, 2, \cdots, r$.

$\Rightarrow (x-y)$ is a common multiple of $m_1, m_2, \cdots, m_r$.

$\Rightarrow [m_1, m_2, \cdots, m_r] \mid (x-y)$

$\Rightarrow x \equiv y \pmod m$

Conversely, $x \equiv y \pmod m \Rightarrow m \mid (x-y)$

$\Rightarrow [m_1 m_2 \cdots m_r] \mid (x-y)$

$\Rightarrow m_i \mid (x-y)$ for $i = 1, 2, \cdots, r$

$\Rightarrow x \equiv y \pmod{m_i}$ for $i = 1, 2, \cdots, r$.

Corollary: If $x \equiv y \pmod{m_1}$ & $x \equiv y \pmod{m_2}$, and $\gcd(m_1, m_2) = 1$, then $x \equiv y \pmod{m_1 m_2}$. $\therefore x-y = s m_1 m_2$

$x - y = q_1 m_1$, $x - y = q_2 m_2$ $\Rightarrow q_1 m_1 = q_2 m_2 \Rightarrow q_2 = q_1 m_1 / m_2 \Rightarrow m_2 | q_1 \Rightarrow q_1 = s \cdot m_2$

Theorem: Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ be a polynomial with $a_i \in \mathbb{Z}$.

If $a \equiv b \pmod m$ then $f(a) \equiv f(b) \pmod m$.

Since $a \equiv b \pmod m$, $a^k \equiv b^k \pmod m$ for $k \in \mathbb{Z}^+$.

$\therefore a_i a^k \equiv a_i b^k \pmod m$, [$\because a_i \in \mathbb{Z}$]

Adding these congruences for $i = 0, 1, 2, \ldots, n$, & for $k = 0, 1, 2, \ldots, n$, we have

$$a_0 + a_1 a + a_2 a^2 + \cdots + a_n a^n \equiv a_0 + a_1 b + a_2 b^2 + \cdots + a_n b^n \pmod m$$

a, $\underline{f(a) \equiv f(b) \pmod m}$.

Divisibility test:

① Let $n = a_m 10^m + a_{m-1} 10^{m-1} + \cdots + a_2 10^2 + a_1 10 + a_0$; where a_k are integers s.t. $0 \le a_k \le 9$, $k = 0, 1, 2, \ldots, m$, be the decimal representation of a positive integer n.

Let $S = a_0 + a_1 + \cdots + a_m$, $T = a_0 - a_1 + \cdots + (-1)^m a_m$.

Then (i) n is divisible by 2 iff a_0 is divisible by 2;

(ii) n " " " 9 " S " " " 9;

(iii) n " " " 11 " T " " " 11.

Proof. (i) Let us consider the polynomial

$$f(x) = a_m x^m + a_{m-1} x^{m-1} + \cdots + a_2 x^2 + a_1 x + a_0$$

$10 \equiv 0 \pmod 2 \Rightarrow f(10) \equiv f(0) \pmod 2$

$\Rightarrow n \equiv a_0 \pmod 2 \Rightarrow \underline{2|n \text{ iff } 2|a_0}$.

$\Rightarrow 2|(n - a_0)$

(ii) $10 \equiv 1 \pmod 9 \Rightarrow f(10) \equiv f(1) \pmod 9$

$\Rightarrow n \equiv S \pmod 9 \Rightarrow 9 | n - S$

$\Rightarrow \underline{9|n \text{ iff } 9|S}$.

(iii) $10 \equiv -1 \pmod{11} \Rightarrow f(10) \equiv f(-1) \pmod{11}$

$\Rightarrow n \equiv T \pmod{11} \Rightarrow 11 | n - T$

$\Rightarrow \underline{11|n \text{ iff } 11|T}$.

eg. Let us consider the number $n = 204568$

$2|n$, since $a_0 = 8$ is divisible by 2

$S = 8+6+5+4+0+2 = 25$ is not divisible by 9.

$T = 8-6+5-4+0-2 = 3$ " " " 11.

eg. Let $n = 456786$ is divisible by 2, 9 & 11.

Since $a_0 = 6$ is divisible by 2

$S = 6+8+7+6+5+4 = 36$ is divisible by 9.

$T = 6-8+7-6+5-4 = 0$ " " " 11.

② Let $n = a_m(100)^m + a_{m-1}(100)^{m-1} + \cdots + a_1(100) + a_0$,
where $a_k \in \mathbb{Z}$ s.t. $0 \le a_k \le 99$; $k = 0, 1, 2, \cdots, m$,
be the representation of a +ve integer n.

Then (i) n is divisible by 2, 4, 5, 10 iff a_0 is divisible by 2, 4, 5, 10.

(ii) n " " " 3 iff S " " " 3.

Example: Let us consider
$$\begin{aligned} n &= 266455 \\ &= 26(100)^2 + 64(100) + 55 \\ &\equiv a_2(100)^2 + a_1(100) + a_0 \end{aligned}$$

Here $a_0 = 55$.

a_0 is divisible by 5 only.

$\therefore n$ " " " 5.

$S = a_0 + a_1 + a_2 = 55 + 64 + 26 = 145$, not divisible by 3.

$\therefore n$ is not divisible by 3.

③. Let $n = a_m(1000)^m + a_{m-1}(1000)^{m-1} + \cdots + a_1(1000) + a_0$;
where a_k are integers s.t. $0 \le a_k \le 999$;

Then (i) $7 | n$ if and only if $7 | T$.

(ii) $13 | n$ " " " " $13 | T$.

(iii) $11 | n$ " " " " $11 | T$.

Example:

① Let us consider $n = 26645249$
$$= 26(1000)^2 + 645(1000) + 249 \equiv a_2(1000)^2 + a_1(1000) + a_0$$

Here $T = a_0 - a_1 + a_2 = 249 - 645 + 26 = -370$

T is not divisible by either 7 or 13 or 11.

$\therefore n$ " " " " " 7 or 13 or 11.

② Let us consider $n = 23146123$
$$= 23(1000)^2 + 146(1000) + 123.$$

$T = a_0 - a_1 + a_2 = 123 - 146 + 23 = 0$, which is divisible by 7, 11, 13.

$\therefore n$ is also divisible by 7, 11, 13.

Fundamental theorem of Arithmetic ; Statement .

Statement

Any positive integer is either 1, or a prime, or it can be expressed as a product of primes, the representation being unique except for the order of the prime factors.

Applications ⟶

① If p be a prime, show that $\sqrt{p}$ is not a rational number

Since p is a prime, $p \geq 2$, $\therefore \sqrt{p} > 1$, for p being a +ve integer.

Let $\sqrt{p}$ be a rational number.

Then $\sqrt{p} = \frac{m}{n}$ for $m, n \in N$.

We assert that $m > 1$, $n > 1$, because

$m = 1, n = 1 \Rightarrow p = 1^2 = 1$, a contradiction ($\because p$ is a prime)

$m > 1, n = 1 \Rightarrow p = m.m$, " " ($\because$ " " ").

$m = 1, n > 1 \Rightarrow \sqrt{p} < 1$, " " ($\because \sqrt{p} > 1$).

$\therefore m > 1, n > 1$.

We have $pn^2 = m^2$.

The number of primes in the factorisation of m – being unique by the fundamental theorem of arithmetic, it follows that the number of primes in the factorisation of m^2 is always even

" " " " of n^2 " " ".

Similarly, " " " " " of pn^2 is odd,

$\therefore$ " " " since p is prime.

Since $pn^2 = m^2$, it appears that the same integer m^2 is expressed as the product of an even number of primes in one representation and as the product of an odd number of primes in another representation.

This contradicts uniqueness of the number of prime factors in the factorization.

$\therefore$ We conclude that $\sqrt{p}$ is not a rational number

Scanned with CamScanner

Ex: Find the least +ve residues in $3^{36} \pmod{77}$.

We have, $3^4 \equiv 4 \pmod{77}$

$\Rightarrow (3^4)^3 \equiv 4^3 \pmod{77} \equiv -13 \pmod{77} \longrightarrow (i)$

$\Rightarrow (3^{12})^2 \equiv (-13)^2 \pmod{77} \equiv 169 \pmod{77}$

$\Rightarrow 3^{24} \equiv 15 \pmod{77} \dashrightarrow (ii)$

from (i) & (ii), we get.

$3^{12} \cdot 3^{24} \equiv (-13) \cdot 15 \pmod{77} \equiv -195 \pmod{77}$

a, $3^{36} \equiv 36 \pmod{77}$

$\therefore$ Least +ve residue in $3^{36} \pmod{77}$ is 36.

Ex: Show that $3^{15} \equiv 1 \pmod{121}$.

$3^5 = 243 = 2 \times 121 + 1$

$\therefore 3^5 \equiv 1 \pmod{121}$

a, $(3^5)^3 \equiv 1^3 \pmod{121}$

a, $3^{15} \equiv 1 \pmod{121}$.

Ex: Find the least +ve residue in $3^{12} \pmod{14}$.

$3^3 = 27 = 2 \times 14 - 1$

$\therefore 3^3 \equiv -1 \pmod{14}$

a, $(3^3)^4 \equiv (-1)^4 \pmod{14}$

a, $3^{12} \equiv 1 \pmod{14}$.

$\therefore$ Least +ve residue in $3^{12} \pmod{14}$ is 1.

Ex: Show that $2^{28} \equiv 3 \pmod{11}$.

$2^4 = 16 \equiv 5 \pmod{11}$

$2^{12} = (2^4)^3 \equiv 5^3 \pmod{11} \equiv 125 \pmod{11} \equiv 4 \pmod{11}$ --- (i)

& $(2^4)^4 = 2^{16} \equiv 5^4 \pmod{11} \equiv 625 \pmod{11} \equiv 9 \pmod{11}$ --- (ii)

$\therefore$ from (i) & (ii), we have,

$2^{12} \cdot 2^{16} = 2^{28} \equiv 4 \cdot 9 \pmod{11} \equiv 36 \pmod{11}$

a, $2^{28} \equiv 3 \pmod{11}$.

STUDY MATERIALS

ON

Congruence Relation

Subject : Mathematics

Paper : GE2T.

Unit – 2.

Dr. Sangita Chakraborty

Associate Professor

Deptt. of Mathematics

Kharagpur College.

Any query at Whatsup No: 9434455417.

NUMBER SYSTEM [Congruence Relation between Integers]

CONGRUENCE → Karl Friedrich Gauss, a German Mathematician introduced this concept which laid the foundation of modern theory of numbers.

Definition → Let m be a fixed positive integer. Two integers a and b are said to be congruent modulo m if $a-b$ is divisible by m.
It is denoted by $a \equiv b \pmod{m}$.

eg. Let $m = 5$; $1 \equiv 6 \pmod 5$, $-4 \equiv 11 \pmod 5$, $10 \equiv 0 \pmod 5$

If $a-b$ is not divisible by m, $a \not\equiv b \pmod m$, then a is said to be incongruent to b modulo m.

eg. $2 \not\equiv 6 \pmod 5$.

Note: when $m = 1$, every two integers are congruent modulo m. So usually m is taken to be a positive integer > 1.

Properties → [Proofs of these properties are given later]

1. $a \equiv a \pmod m$ → reflexive
2. If $a \equiv b \pmod m$, then $b \equiv a \pmod m$ → Symmetric.
3. If $a \equiv b \pmod m$, and $b \equiv c \pmod m$, then $a \equiv c \pmod m$ → transitive
4. If $a \equiv b \pmod m$, then for any $c \in \mathbb{Z}$,
$$a + c \equiv (b+c) \pmod m$$
$$a \cdot c \equiv b \cdot c \pmod m$$
5. If $a \equiv b \pmod m$, and $c \equiv d \pmod m$, then
$$a \pm c \equiv (b \pm d) \pmod m$$
$$a \cdot c \equiv b \cdot d \pmod m$$
6. If $a \equiv b \pmod m$ and $d | m$, $d > 0$, then $a \equiv b \pmod d$

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

By Division algorithm $\exists\, q \in \mathbb{Z}, r \in \mathbb{Z}$ s.t.
$$a = q \cdot m + r, \quad 0 \le r < m.$$
Since $a - r = q \cdot m \Rightarrow a \equiv r \pmod m$
$\Rightarrow r$ is a residue of a modulo m.

r is said to be the least non-negative residue of a modulo m.

The whole set $\mathbb{Z}$ of integers is divided into only m distinct and disjoint subsets, called the residue classes modulo m, denoted by

$\bar{0} = \{0, \pm m, \pm 2m, \ldots\} = \{mk : k \in \mathbb{Z}\}$

$\bar{1} = \{1, 1 \pm m, 1 \pm 2m, \ldots\} = \{mk+1 : k \in \mathbb{Z}\}$

$\ldots$

$\{mk + (m-1) : k \in \mathbb{Z}\} = \overline{m-1} = \{m-1, (m-1) \pm m, (m-1) \pm 2m, \ldots\}$

[Any two integers in a residue class are congruent modulo m whereas they are not when belonging to different residue classes]

Theorem: For any $a \in \mathbb{Z}, b \in \mathbb{Z}$, $a \equiv b \pmod m$ if and only if a and b leaves the same remainder when divided by m.

Proof: Let r be the remainder when a is divided by m. Then $\exists$ some $q \in \mathbb{Z}$ s.t. $a = q \cdot m + r$, $0 \le r < m$.

Since $a \equiv b \pmod m$, $a - b = K \cdot m$, $K \in \mathbb{Z}$.

$\Rightarrow b = a - K \cdot m = (q - K) \cdot m + r$

$\Rightarrow$ b leaves the same remainder r, when divided by m.

Conversely, let r be the same remainder when a and b are divided by m. Then $\exists$ some $q_1, q_2 \in \mathbb{Z}$ s.t. $a = q_1 m + r$, $b = q_2 \cdot m + r$

$\Rightarrow a - b = (q_1 - q_2) \cdot m \Rightarrow m \mid a - b \Rightarrow a \equiv b \pmod m$.

eg. $34 \equiv 4 \pmod 6$; $34 = 5 \cdot 6 + 4$, $4 = 0 \cdot 6 + 4$

Theorem: If $a \equiv b \pmod m$ then $a^n \equiv b^n \pmod m$, $\forall n \in \mathbb{Z}^+$.

We use the principle of Mathematical Induction to prove the theorem.

The Theorem is true for $n = 1$.

Let us assume that the theorem is true for some $K \in \mathbb{Z}^+$. Then $a^K \equiv b^K \pmod m$.

Now $a^K \equiv b^K \pmod m$ and $a \equiv b \pmod m$ together

$\Rightarrow a^K \cdot a \equiv b^K \cdot b \pmod m$

$\Rightarrow a^{K+1} \equiv b^{K+1} \pmod m$.

$\therefore$ The theorem is true for the positive integer $K+1$ if we assume it to be true for $K \in \mathbb{Z}^+$.

$\therefore$ By the principle of Induction,

$$a^n \equiv b^n \pmod m, \ \forall n \in \mathbb{Z}^+.$$

Alternatively, $a^K \equiv b^K \pmod m \Rightarrow a^K - b^K = q_1 m$, $q_1 \in \mathbb{Z}$.

$a \equiv b \pmod m \Rightarrow a - b = q_2 \cdot m$, $q_2 \in \mathbb{Z}$.

Now, $a \cdot (a^K - b^K) = (a \cdot q_1) \cdot m$, and $b^K \cdot (a - b) = (b^K q_2) \cdot m$

$\Rightarrow a \cdot (a^K - b^K) + b^K \cdot (a - b) = (a q_1 + b^K q_2) \cdot m$

$\Rightarrow a^{K+1} - \cancel{a b^K} + \cancel{a b^K} - b^{K+1} = (a q_1 + b^K q_2) \cdot m$

$\Rightarrow a^{K+1} - b^{K+1} = (a q_1 + b^K q_2) \cdot m$

$\Rightarrow a^{K+1} \equiv b^{K+1} \pmod m$

The Converse is NOT True:-

example, $3^2 \equiv 5^2 \pmod 4$ but $3 \not\equiv 5 \pmod 4$

$5^3 \equiv 8^3 \pmod 9$ but $5 \not\equiv 8 \pmod 9$.

Proof of the properties of Congruence Relation :-

① $a \equiv a \pmod m$ $\rightarrow$ reflexive property

<u>Proof</u>: $a-a$ is divisible by m, where m be a fixed +ve integer.

i.e., $a \equiv a \pmod m$.

② If $a \equiv b \pmod m$, then $b \equiv a \pmod m$ $\rightarrow$ Symmetric prop.

<u>Proof</u>: $a \equiv b \pmod m \Rightarrow a-b$ is divisible by m.

$\Rightarrow b-a$ " " " m.

$\Rightarrow b \equiv a \pmod m$.

③ If $a \equiv b \pmod m$ and $b \equiv c \pmod m$, then $a \equiv c \pmod m$.

This is transitive prop.

<u>Proof</u>: $a \equiv b \pmod m$ & $b \equiv c \pmod m$

$\Rightarrow m \mid (a-b)$ & $m \mid (b-c)$

$\Rightarrow a-b = K_1 m$ & $b-c = K_2 m$; $K_1, K_2 \in \mathbb{Z}$.

Now $a-c = (a-b)+(b-c) = (K_1+K_2) \cdot m$; $K_1+K_2 \in \mathbb{Z}$.

$\Rightarrow m \mid a-c \Rightarrow a \equiv c \pmod m$.

<u>Remarks</u>:

Therefore, from ①, ② & ③, it is understood that Congruence relation is an equivalence relation.

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

(i) $a+c \equiv (b+c) \pmod m$; (ii) $a \cdot c \equiv b \cdot c \pmod m$.

<u>Proof</u>: (i) $a \equiv b \pmod m \Rightarrow m \mid (a-b) \Rightarrow a-b = K \cdot m$; $K \in \mathbb{Z}$.

Now, $(a+c)-(b+c) = a-b = K \cdot m$

$\therefore a+c \equiv (b+c) \pmod m$.

(ii) $a \cdot c - b \cdot c = (a-b) \cdot c = K m \cdot c = (Kc) \cdot m$; $Kc \in \mathbb{Z}$.

$\Rightarrow a \cdot c \equiv b \cdot c \pmod m$.

⑤ If $a \equiv b \pmod m$, and $c \equiv d \pmod m$, then

(i) $a \pm c \equiv (b \pm d) \pmod m$; (ii) $a \cdot c \equiv b \cdot d \pmod m$

<u>Proof</u>; (i) $a \equiv b \pmod m \Rightarrow m \mid (a-b) \Rightarrow a-b = K_1 m$, $K_1 \in$

$c \equiv d \pmod m \Rightarrow m \mid (c-d) \Rightarrow c-d = K_2 m$, $K_2 \in$

Now $a \pm c = (b+K_1 m) \pm (d+K_2 m) = (b \pm d) + (K_1 \pm K_2) \cdot m$

$\Rightarrow (a \pm c) - (b \pm d) = (K_1 \pm K_2) \cdot m \Rightarrow a \pm c \equiv (b \pm d) \pmod m$

(ii) $a \cdot c = (b+K_1 m) \cdot (d+K_2 m) = bd + (bK_2 + dK_1 + K_1 K_2 m) \cdot m$

$\Rightarrow a \cdot c - b \cdot d = (bK_2 + dK_1 + K_1 K_2 m) \cdot m \Rightarrow a \cdot c \equiv b \cdot d \pmod m$.

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

Proof: $a \equiv b \pmod{m} \Rightarrow m | (a-b) \Rightarrow a-b = Km$; $K \in \mathbb{Z}$.

And $d | m \Rightarrow m = r.d$; $r \in \mathbb{Z}$.

$\therefore$ $a-b = Km = K(r.d) = (Kr) \cdot d$; $Kr \in \mathbb{Z}$.

$\Rightarrow d | (a-b) \Rightarrow \underline{a \equiv b \pmod{d}}$.

Ex: Prove that if f be a polynomial with integral coefficients and if $f(a) \equiv K \pmod{m}$, then $f(a+m) \equiv K \pmod{m}$.

Let $f(x) = c_0 + c_1 x + c_2 x^2 + \cdots + c_n x^n$; $c_i \in \mathbb{Z}, \forall i$

$f(a) = c_0 + c_1 a + c_2 a^2 + \cdots + c_n a^n$

& $f(a+m) = c_0 + c_1(a+m) + \cdots + c_n(a+m)^n$.

$= (c_0 + c_1 a + c_2 a^2 + \cdots + c_n a^n) + m.q$; $q \in \mathbb{Z}$.

$\therefore$ $f(a+m) = f(a) + m.q \equiv f(a) \pmod{m} + 0 \pmod{m}$,

$\Rightarrow f(a+m) \equiv f(a) \pmod{m}$, since $m.q \equiv 0 \pmod{m}$.

$\therefore$ $\underline{f(a+m) \equiv K \pmod{m}}$. , since $f(a) \equiv K \pmod{m}$.

Ex: Use the theory of congruences to prove:

(i) $7 \mid (2^{5n+3} + 5^{2n+3})$; $\forall n \geq 1, n \in \mathbb{Z}$.

(ii) $43 \mid (6^{n+2} + 7^{2n+1})$; $\forall n \geq 1, n \in \mathbb{Z}$.

(iii) $17 \mid (2^{3n+1} + 3.5^{2n+1})$; $\forall n \geq 1, n \in \mathbb{Z}$.

Solution:

(i) $2^{5n+3} + 5^{2n+3} = 2^3.(2^5)^n + 5^3.(5^2)^n = 8.32^n + 125.25^n$.

Now, $32 \equiv 25 \pmod 7$

$\Rightarrow 32^n \equiv 25^n \pmod 7$, $\forall n \geq 1$. [using the fact; $a \equiv b \pmod m \Rightarrow a^n \equiv b^n \pmod m$]

or, $8.32^n \equiv 8.25^n \pmod 7$, by property ④.

$\Rightarrow 8.32^n - 8.25^n \equiv 0 \pmod 7 \longrightarrow$ ①

Also we have, $133.25^n \equiv 0 \pmod 7 \longrightarrow$ ②

$\therefore$ From ① & ②, we get

$8.32^n - 8.25^n + 133.25^n \equiv 0 \pmod 7$, by prop ⑤:

or, $8.32^n + 125.25^n \equiv 0 \pmod 7$

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

(ii) $6^{n+2} + 7^{2n+1} = 6^2.6^n + 7.(7^2)^n = 36.6^n + 7.49^n$.

Now $6 \equiv 49 \pmod{43}$

$\Rightarrow 6^n \equiv 49^n \pmod{43}$, $\forall n \geq 1 \longrightarrow$ ①.

$\Rightarrow 36.6^n - 36.49^n \equiv 0 \pmod{43} \longrightarrow$ ②.

Also, $43.49^n \equiv 0 \pmod{43}$

From ① & ②, we get

$36.6^n - 36.49^n + 43.49^n \equiv 0 \pmod{43}$

or, $6^2.6^n + 7.49^n \equiv 0 \pmod{43}$

$\Rightarrow 43 \mid (6^{n+2} + 7^{2n+1})$, $\forall n \geq 1$.

(iii) $2^{3n+1} + 3.5^{2n+1} = 2.8^n + 3.5.25^n$

Now $8 \equiv 25 \pmod{17}$

$\Rightarrow 8^n \equiv 25^n \pmod{17}, \quad \forall n \geq 1.$

or, $2.8^n - 2.25^n \equiv 0 \pmod{17} \longrightarrow (1).$

Also, $17.25^n \equiv 0 \pmod{17} \longrightarrow (2).$

From (1) & (2), we get

$$2.8^n - 2.25^n + 17.25^n \equiv (0+0) \pmod{17}$$

or, $2.8^n + 15.25^n \equiv 0 \pmod{17}$

i.e., $17 \mid (2^{3n+1} + 3.5^{2n+1}).$

Ex: Prove that $1! + 2! + \cdots + 1000! \equiv 3 \pmod{15}$.

Now, $(5+n)! \equiv 0 \pmod{15}$ for $n \geq 0, n \in \mathbb{Z}$.

Again, $1! + 2! + 3! + 4! = 33 \equiv 3 \pmod{15}$

$\therefore (1! + 2! + 3! + 4!) + (5! + 6! + \cdots + 1000!)$

$\equiv 3 \pmod{15} + 0 \pmod{15}$

$\equiv 3 \pmod{15}.$ (proved)

Ex: Find the remainder when $1! + 2! + 3! + \cdots + 100!$ is divided by 24.

$4! \equiv 0 \pmod{24}$, and for any +ve integer n, $(4+n)! \equiv 0 \pmod{24}$.

Therefore, $1! + 2! + 3! + 4! + \cdots + 100!$

$\equiv (1! + 2! + 3!) \pmod{24}$

$\equiv 9 \pmod{24}.$

$\therefore$ the remainder is $\underline{9}$.

Theorem: If $a.x \equiv a.y \pmod m$ and $\gcd(a,m)=1$, then $x \equiv y \pmod m$

Proof: $ax - ay = q.m$, $q \in \mathbb{Z}$.

$\Rightarrow x - y = \frac{q.m}{a}$. Since $x-y$ is an integer, $\therefore a \mid q.m$.

Since $\gcd(a,m)=1$, $\therefore a \mid q \Rightarrow q = K.a$, $K \in \mathbb{Z}$.

$\therefore x - y = \frac{K.a.m}{a} = K.m \Rightarrow x \equiv y \pmod m$.

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

We have $ax - ay = q.m$, $q \in \mathbb{Z}$.

Since $\gcd(a,m) = d$, $a = d.r$, $m = d.s$; $r, s \in \mathbb{Z}$, and prime to each other

$\therefore d.r.x - d.r.y = q.d.s$

$\Rightarrow r.(x-y) = q.s \Rightarrow x - y = \frac{q.s}{r}$

Since $x-y$ is an integer, $r \mid q.s \Rightarrow r \mid q$, since $\gcd(r,s)=1$.

i.e., $\frac{q}{r}$ is an integer, say, K.

$\therefore x - y = K.s = K.\left(\frac{m}{d}\right) \Rightarrow x \equiv y \pmod{\frac{m}{d}}$.

Conversely. Let $x \equiv y \pmod{\frac{m}{d}}$. $\Rightarrow \frac{m}{d} \mid (x-y)$

$\Rightarrow m \mid d(x-y) \Rightarrow m \mid a(x-y)$

$\Rightarrow ax \equiv ay \pmod m$.

Corollary: If $ax = ay \pmod m$ and $a \mid m$ then $x \equiv y \pmod{\frac{m}{a}}$.

$ax - ay = q.m$, for $q \in \mathbb{Z}$.

$x - y = \frac{qm}{a} = K.q$ [where $\frac{m}{a} = K \in \mathbb{Z}$, since $a \mid m$]

$\therefore x \equiv y \pmod K \Rightarrow x \equiv y \pmod{\frac{m}{a}}$.

Theorem: $x \equiv y \pmod{m_i}$, for $i = 1, 2, \dots, r$
$\Leftrightarrow x \equiv y \pmod m$, where $m = [m_1, m_2, \dots, m_r]$, the l.c.m. of m_i's. $i = 1, 2, \dots, r$.

$x \equiv y \pmod{m_i} \Rightarrow m_i \mid (x-y)$, for $i = 1, 2, \dots, r$.

$\Rightarrow (x-y)$ is a common multiple of $m_1, m_2, \dots, m_r$.

$\Rightarrow [m_1, m_2, \dots, m_r] \mid (x-y)$

$\Rightarrow x \equiv y \pmod m$

Conversely, $x \equiv y \pmod m \Rightarrow m \mid (x-y)$

$\Rightarrow [m_1 m_2 \dots m_r] \mid (x-y)$

$\Rightarrow m_i \mid (x-y)$ for $i = 1, 2, \dots, r$

$\Rightarrow x \equiv y \pmod{m_i}$ for $i = 1, 2, \dots, r$.

Corollary: If $x \equiv y \pmod{m_1}$ & $x \equiv y \pmod{m_2}$, and $\gcd(m_1, m_2) = 1$, then $x \equiv y \pmod{m_1 m_2}$. $\therefore x - y = s\, m_1 m_2$

$\left.\begin{array}{l} x-y = q_1 m_1 \\ x-y = q_2 m_2 \end{array}\right\} \Rightarrow q_1 m_1 = q_2 m_2 \Rightarrow q_2 = q_1 m_1 / m_2 \Rightarrow m_2 | q_1 \Rightarrow q_1 = s.m_2$

Theorem: Let $f(x) = a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$ be a polynomial with $a_i \in \mathbb{Z}$.

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

Since $a \equiv b \pmod m$, $a^K \equiv b^K \pmod m$ for $K \in \mathbb{Z}^+$.

$\therefore a_i a^K \equiv a_i b^K \pmod m$, $[\because a_i \in \mathbb{Z}]$ for $i = 0, 1, 2, \ldots, n$,

Adding these congruences & for $K = 0, 1, 2, \ldots, n$, we have

$$a_0 + a_1 a + a_2 a^2 + \cdots + a_n a^n \equiv a_0 + a_1 b + a_2 b^2 + \cdots + a_n b^n \pmod m$$

a, $\underline{f(a) \equiv f(b) \pmod m}$.

Divisibility test:

① Let $n = a_m 10^m + a_{m-1} 10^{m-1} + \cdots + a_2 10^2 + a_1 10 + a_0$; where a_K are integers s.t. $0 \le a_K \le 9$, $K = 0, 1, 2, \ldots, m$, be the decimal representation of a positive integer n.

Let $S = a_0 + a_1 + \cdots + a_m$, $T = a_0 - a_1 + \cdots + (-1)^m a_m$.

Then (i) n is divisible by 2 iff a_0 is divisible by 2;

(ii) n " " " 9 " S " " " 9;

(iii) n " " " 11 " T " " " 11.

Proof. (i) Let us consider the polynomial

$$f(x) = a_m x^m + a_{m-1} x^{m-1} + \cdots + a_2 x^2 + a_1 x + a_0$$

$10 \equiv 0 \pmod 2 \Rightarrow f(10) \equiv f(0) \pmod 2$

$\Rightarrow n \equiv a_0 \pmod 2 \Rightarrow \underline{2 | n \text{ iff } 2 | a_0}$.

$\Rightarrow 2 | (n - a_0)$

(ii) $10 \equiv 1 \pmod 9 \Rightarrow f(10) \equiv f(1) \pmod 9$

$\Rightarrow n \equiv S \pmod 9 \Rightarrow 9 | n - S$

$\Rightarrow \underline{9 | n \text{ iff } 9 | S}$.

(iii) $10 \equiv -1 \pmod{11} \Rightarrow f(10) \equiv f(-1) \pmod{11}$

$\Rightarrow n \equiv T \pmod{11} \Rightarrow 11 | n - T$

$\Rightarrow \underline{11 | n \text{ iff } 11 | T}$.

eg. Let us consider the number $n = 204568$

$2 | n$, since $a_0 = 8$ is divisible by 2

$S = 8+6+5+4+0+2 = 25$ is not divisible by 9

$T = 8-6+5-4+0-2 = 3$ " " " " 11.

eg. Let $n = 456786$ is divisible by 2, 9 & 11.

Since $a_0 = 6$ is divisible by 2

$S = 6+8+7+6+5+4 = 36$ is divisible by 9.

$T = 6-8+7-6+5-4 = 0$ " " " 11.

② Let $n = a_m(100)^m + a_{m-1}(100)^{m-1} + \cdots + a_1(100) + a_0$,
where $a_k \in \mathbb{Z}$ s.t. $0 \le a_k \le 99$; $k = 0, 1, 2, \cdots, m$,
be the representation of a +ve integer n.
Then (i) n is divisible by 2, 4, 5, 10 iff a_0 is divisible by 2, 4, 5, 10.
(ii) n " " " 3 iff S " " " 3.

Example: Let us consider
$n = 266455$
$= 26(100)^2 + 64(100) + 55$
$\equiv a_2(100)^2 + a_1(100) + a_0$

Here $a_0 = 55$.
a_0 is divisible by 5 only.
$\therefore$ n " " " 5.
$S = a_0 + a_1 + a_2 = 55 + 64 + 26 = 145$, not divisible by 3.
$\therefore$ n is not divisible by 3.

③. Let $n = a_m(1000)^m + a_{m-1}(1000)^{m-1} + \cdots + a_1(1000) + a_0$;
where a_k are integers s.t. $0 \le a_k \le 999$;
Then (i) $7 \mid n$ if and only if $7 \mid T$.
(ii) $13 \mid n$ " " " " $13 \mid T$.
(iii) $11 \mid n$ " " " " $11 \mid T$.

Example:

① Let us consider $n = 26645249$
$= 26(1000)^2 + 645(1000) + 249 \equiv a_2(1000)^2 + a_1(1000) + a_0$

Here $T = a_0 - a_1 + a_2 = 249 - 645 + 26 = -370$
T is not divisible by either 7 or 13 or 11.
$\therefore$ n " " " " " 7 or 13 or 11.

② Let us consider $n = 23146123$
$= 23(1000)^2 + 146(1000) + 123$.
$T = a_0 - a_1 + a_2 = 123 - 146 + 23 = 0$, which is divisible by 7, 11, 13.
$\therefore$ n is also divisible by 7, 11, 13.

Ex: Find the least +ve residues in $3^{36} \pmod{77}$.

We have, $3^4 \equiv 4 \pmod{77}$

$\Rightarrow (3^4)^3 \equiv 4^3 \pmod{77} \equiv -13 \pmod{77} \longrightarrow (i)$

$\Rightarrow (3^{12})^2 \equiv (-13)^2 \pmod{77} \equiv 169 \pmod{77}$

$\Rightarrow 3^{24} \equiv 15 \pmod{77} \dashrightarrow (ii)$

from (i) & (ii), we get.

$3^{12} \cdot 3^{24} \equiv (-13) \cdot 15 \pmod{77} \equiv -195 \pmod{77}$

a, $3^{36} \equiv 36 \pmod{77}$

$\therefore$ Least +ve residue in $3^{36} \pmod{77}$ is 36.

Ex: Show that $3^{15} \equiv 1 \pmod{121}$.

$3^5 = 243 = 2 \times 121 + 1$

$\therefore 3^5 \equiv 1 \pmod{121}$

a, $(3^5)^3 \equiv 1^3 \pmod{121}$

a, $3^{15} \equiv 1 \pmod{121}$.

Ex: Find the least +ve residue in $3^{12} \pmod{14}$.

$3^3 = 27 = 2 \times 14 - 1$

$\therefore 3^3 \equiv -1 \pmod{14}$

a, $(3^3)^4 \equiv (-1)^4 \pmod{14}$

a, $3^{12} \equiv 1 \pmod{14}$.

$\therefore$ Least +ve residue in $3^{12} \pmod{14}$ is 1.

Ex: Show that $2^{28} \equiv 3 \pmod{11}$.

$2^4 = 16 \equiv 5 \pmod{11}$

$2^{12} = (2^4)^3 \equiv 5^3 \pmod{11} \equiv 125 \pmod{11} \equiv 4 \pmod{11}$ --- (i)

& $(2^4)^4 = 2^{16} \equiv 5^4 \pmod{11} \equiv 625 \pmod{11} \equiv 9 \pmod{11}$ --- (ii)

$\therefore$ from (i) & (ii), we have,

$2^{12} \cdot 2^{16} = 2^{28} \equiv 4 \cdot 9 \pmod{11} \equiv 36 \pmod{11}$

a, $2^{28} \equiv 3 \pmod{11}$.

Fundamental theorem of Arithmetic ; Statement.

Statement.

Any positive integer is either 1, or a prime, or it can be expressed as a product of primes, the representation being unique except for the order of the prime factors.

Applications →

① If p be a prime, show that $\sqrt{p}$ is not a rational number.

Since p is a prime, $p \geq 2$, $\therefore \sqrt{p} > 1$, for p being a +ve integer.

Let $\sqrt{p}$ be a rational number.

Then $\sqrt{p} = \frac{m}{n}$ for $m, n \in N$.

We assert that $m > 1$, $n > 1$, because

$m = 1,\ n = 1 \Rightarrow p = 1^2 = 1$, a contradiction ($\because p$ is a prime)

$m > 1,\ n = 1 \Rightarrow p = m.m$, " " ($\because$ " " ")

$m = 1,\ n > 1 \Rightarrow \sqrt{p} < 1$, " " ($\because \sqrt{p} > 1$).

$\therefore$ $m > 1$, $n > 1$.

We have $pn^2 = m^2$.

The number of primes in the factorisation of m being unique by the fundamental theorem of arithmetic, it follows that the number of primes in the factorisation of m^2 is always even

" " " " " of n^2 " " ".

Similarly, " " " " " of pn^2 is odd,

$\therefore$ " " " since p is prime.

Since $pn^2 = m^2$, it appears that the same integer m^2 is expressed as the product of an even number of primes in one representation and as the product of an odd number of primes in another representation.

This contradicts uniqueness of the number of prime factors in the factorization.

$\therefore$ We conclude that $\sqrt{p}$ is not a rational number.