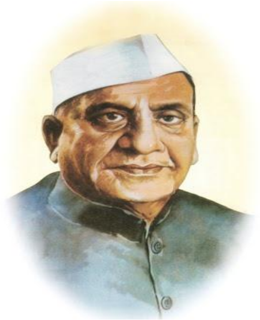

Mahatma Fule Arts, Commerce, and Sitaramji Chaudhari Science Mahavidyalaya, Warud

Department of Mathematics

Congruence classes

Dr. R. S. Wadbude

Associate Professor

Contents

Congruence modulo m

Let m be any fixed positive integer i.e. $m > 0$. Then an integer a is said to be congruent to another integer b modulo m if $m \mid a - b$.

Denoted by $a \equiv b \pmod{m}$

and read a is congruent to b modulo m

$$
\begin{aligned}
a \equiv b \pmod{m} &\Leftrightarrow m \mid a - b \\
&\Leftrightarrow m \mid -(b - a) \\
&\Leftrightarrow (a-b) \text{ is multiple of 'm'} \\
&\Leftrightarrow m \text{ divides } (a-b)
\end{aligned}
$$

Examples:

$$
\begin{aligned}
89 \equiv 25 \pmod{4} &\Leftrightarrow 4 \mid 89 - 25 &&\Leftrightarrow 4 \mid 64 \\
153 \equiv -7 \pmod{8} &\Leftrightarrow 8 \mid 153 + 7 &&\Leftrightarrow 8 \mid 160 \\
13 \equiv 3 \pmod{5} &\Leftrightarrow 5 \mid 13 - 3 &&\Leftrightarrow 5 \mid 10
\end{aligned}
$$

Equivalence Relation

Theorem : The congruence is an equivalence relation. That is, we have:

1. $a \equiv a \pmod{m}$ (Reflexive)
2. $a \equiv b \pmod{m} \Rightarrow b \equiv a \pmod{m}$ (Symmetric)
3. $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m} \Rightarrow a \equiv c \pmod{m}$ (Transitive)

Residue or Congruence classes

Definition:

Let M be a fixed positive integer, then ‘congruence modulo m’ is an equivalence Relation in the set of integers. Consequently it will be partition I into equivalence classes. These equivalence classes are called residue or congruence classes modulo m. Denoted the set of all residue classes of integers modulo m by $\mathbf{I_m}$.

If $a \in \mathbf{I}$ then the residue class $[a] \in \mathbf{I_m}$

$$[a] = \{ x : x \in I \text{ and } x \equiv a \pmod{m} \} \quad \text{i.e } m \mid x - a$$

Similarly

If $b \in \mathbf{I_m}$ then the residue class $[b] \in \mathbf{I_m}$

$$[b] = \{ y : y \in I \text{ and } y \equiv b \pmod{m} \} \quad \text{i.e } m \mid y - b$$

➢Two equivalence classes are either disjoint or identical.

i.e. $[a] = [b]$ or $[a] \cap [b] = \phi \quad \forall\, [a], [b] \in I_m$

➢ If $[a] = [b]$ if and only if $a \equiv b \pmod{m}$ if and only if $m \mid a - b$

Thus

$[a] = [a \pm m] = [a \pm 2m] = [a \pm 3m] = [a \pm 4m] \ldots$

Example: The residue classes for modulo 4 i.e. The elements of set I_4

[0] = {…, - 12, - 8, - 4, 0, 4, 8, 12, …}

[1] = { …,- 15, - 11, - 7, - 3, 1, 5, 9, 13, …}

[2] = {…,- 14, -10, - 6, 2, 6, 10, 14, 18, …}

[3] = { …, 13, - 9, - 5, - 1, 3, 7, 11, 15, 19, …}

Obviously [0] = [4] = [8] ….. and [1] = [5] = [9] = [13]……

The basic properties of residue classes modulo m:

1. If a and b are elements of the same residue classes [s] , then $a \equiv b \pmod m$.
2. If [s] and [t] are two distinct with residue classes $a \in [s]$ and $b \in [t]$,

   then a and b are incongruent modulo m.
3. Two integers x and y are in the same residue class if and only if $x \equiv y \pmod m$,
4. The m residue classes $[0]m, [1]m, \ldots, [m - 1]m$ are disjoint and their union is

   the set of all integers.

Theorem 1:
Every integer is congruent (mod m) to exactly one of the numbers in the list : 0, 1, 2, ……. (m - 2), (m -1).

Theorem 2.
$ca \equiv cb \pmod m$ implies $a \equiv b \pmod m$ if and only if $(c, m) = 1$.

Theorem :

The set $\mathbf{I_m}$ of all residue classes of integer modulo m contains exactly m distinct elements .

Proof:

We claim that $\mathbf{I_m} = \{ [0], [1], [2]....[m-1]\}$. First we show that m residue classes are all distinct. Let $0 \le i < m$, $0 \le j < m$, and $j > i$.

Then $[i] = [j] \Rightarrow i \equiv j \pmod m \Rightarrow$ i - j is divisible by m $\Rightarrow$ j - i is divisible by m.

But j – i is a positive integer less than m. So it can not be divisible by m.

Therefore $[i] \neq [j]$ and [0], [1], [2]….[m-1] are all distinct.

Now we shall show that if a is any integer, then the residue class [a] is equal to one of the residue classes [0], [1], [2]….[m-1]

by DAT, we have

$a = km + r$, where $k, r \in I$ and $0 \le r < m$

$\Rightarrow a - r = km$

$\Rightarrow$ a –r divisible by m

$\Rightarrow a \equiv r \pmod{m}$

$\Rightarrow [a] = [r]$

Since $0 \leq r \leq m - 1$, therefore the residue class $[a] = [r]$ is one of the classes

[0], [1], [2]....[m-1]

Hence the set $\mathbf{I_m}$ has m distinct elements.

THANK YOU