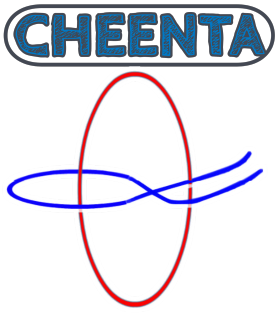

Cheenta

IOQM Concepts Revisited

Created By :
J V Raghunath

Topic : Basics of Congruences and its Properties

Overview

We will learn about,

1. Basics of Congruences
2. Properties of Congruences
3. Problems involving Congruences

1 Basics of Congruences

For a fixed positive integer n and $a, b \in \mathbb{Z}$, we say a and b are *congrunt modulo* n, i.e.,

$$a \equiv b \pmod{n} \iff n \mid (a-b)$$

that is, if and only if $a - b = kn$, for some $k \in \mathbb{Z}$.
For example, $5 \equiv 40 \pmod{7},\ 4 \equiv 40 \pmod{6},\ 26 \not\equiv 11 \pmod{7}$.

Lemma 1.1. *Given $n \in \mathbb{N}$, then any integer is congruent to its remainder when divided by n and not to any other non-negative number less than n, when considered under* (mod n).

Proof. Given $a, n \in \mathbb{Z}$, by the *Division Algorithm*, there exist $q, r \in \mathbb{Z}$, such that,

$$a = nq + r, \text{ where } 0 \leq r < n$$

$\implies n \mid (a-r) \implies a \equiv r \pmod{n}$, where r is the remainder when a is divided by n. To prove the uniqueness of the value of $r < n$, suppose consider $a \equiv r_1 \pmod{n}$, for some $0 \leq r_1 < n$
$\implies n \mid (a - r_1) \implies a - r_1 = nq_1$, for some $q_1 \in \mathbb{Z} \implies a = nq_1 + r_1$
But by the *Division Algorithm*, we know that such a value of r_1 is unique which is the remainder of a when divided by $n \implies r_1 = r$. Hence proved □

So, any integer is congruent (mod n) to exactly one of $\{0, 1, 2, \ldots, n-1\}$.

- The set of n integers $\{0, 1, 2, \ldots, n-1\}$ is called as the *set of least non-negative residues modulo n.*
- The set of n integers which is congruent to $\{0, 1, 2, \ldots, n-1\}$ in some order is called a *complete set of residues modulo n.* For example, $\{-2, -8, 13, 7\}$ forms a complete set of residues modulo 4, because it is congruent to $\{2, 0, 1, 3\}$ in the same order which is nothing but $\{0, 1, 2, 3\}$.

Theorem 1.1. *For any $n \in \mathbb{N}$ and $a, b \in \mathbb{Z}$,*

$$a \equiv b \pmod{n} \iff a \text{ and } b \text{ leave the same remainder when divided by "}n\text{".}$$

Proof. Suppose, $a \equiv b \pmod{n} \implies a - b = kn$, for some $k \in \mathbb{Z} \implies a = kn + b$. By the *Division Algorithm*, $b = qn + r$, where r is the remainder when b is divided by $n \implies a = (k+q)n + r$, hence again by the *Division Algorithm*, since the remainder must be unique, r is also the remainder when a is divided by n. Hence, a and b leave the same remainder when divided by "n".
Conversely, suppose a and b leave the same remainder when divided by "n", say r. Then by the *Division Algorithm*, $a = q_1 n + r \ ; \ b = q_2 n + r \implies a - b = (q_1 - q_2)n \implies n \mid (a - b) \implies a \equiv b \pmod{n}$. □

2 Properties of Congruences

Here $a, b, c, d \in \mathbb{Z}$ and $n, k \in \mathbb{N}$,

- $a \equiv a \pmod{n}$ [Reflexivity]
- $a \equiv b \pmod{n} \iff b \equiv a \pmod{n}$ [Symmetry]
- If $a \equiv b$ and $b \equiv c \implies a \equiv c \pmod{n}$ [Transitivity]
- If $a \equiv b$ and $c \equiv d \implies a + c \equiv b + d \pmod{n}$ [Addition]
- If $a \equiv b$ and $c \equiv d \implies ac \equiv bd \pmod{n}$ [Multiplication]

  Proof. So we have, $a - b = nk_1 \ ; \ c - d = nk_2$. Multiply by "$c$" in the first equation and by "b" in the second equation and add the both to get, $ac - bd = n(ck_1 + bk_2) \implies n \mid (ac - bd) \implies ac \equiv bd \pmod{n}$ □

- If $a \equiv b \pmod{n} \implies a^k \equiv b^k \pmod{n}$. The converse is NOT TRUE

  Proof. Obviously, $a^1 \equiv b^1 \pmod{n}$ which is given. Suppose,

  $$\begin{aligned} a^{m-1} \equiv b^{m-1} \pmod{n} &\implies a^{m-1} \cdot a \equiv b^{m-1} \cdot b \pmod{n} \ (\because a \equiv b) \\ &\implies a^m \equiv b^m \pmod{n}. \end{aligned}$$

  Hence, by the *First Principle of Finite Induction*, $a^k \equiv b^k, \forall k \in \mathbb{N}$.
  The converse is not true because there are many counter examples such as, $2^2 \equiv 8^2 \pmod{4}$, but $2 \not\equiv 8 \pmod{4}$. □

- For $c \neq 0$, $ca \equiv cb \pmod{n} \iff a \equiv b \left(\mod \frac{n}{\mathrm{GCD}(c,n)}\right)$

  Proof. Suppose, $ca \equiv cb \pmod{n} \implies n \mid c(a-b)$.
  Let $\mathrm{GCD}(c,n) = d \implies \mathrm{GCD}(\frac{c}{d}, \frac{n}{d}) = 1$.
  Then $\frac{n}{d} \mid \frac{c}{d}(a-b)$, but since $\frac{c}{d}$ and $\frac{n}{d}$ are relatively prime, by the *Euclid's Lemma*, $\frac{n}{d} \mid (a-b) \implies a \equiv b \pmod{\frac{n}{d}}$.
  Conversely, suppose that,

$$\begin{aligned} & a \equiv b \left(\mod \frac{n}{\mathrm{GCD}(c,n)}\right) \\ \implies & \frac{n}{\mathrm{GCD}(c,n)} \mid (a-b) \\ \implies & n \mid \mathrm{GCD}(c,n)(a-b) \\ \implies & n \mid c(a-b) \text{ (Since } c \text{ is a multiple of } \mathrm{GCD}(c,n)) \\ \implies & ca \equiv cb \pmod{n} \end{aligned}$$

  □

3 Problems involving Congruences

Question 3.1. *Let n be a positive integer and let $a_1, a_2, a_3, \ldots, a_k$ (here $k \geq 2$) be distinct integers in the set $\{1, 2, \ldots, n\}$ such that n divides $a_i\,(a_{i+1} - 1)$ for $i = 1, 2, \ldots, k-1$. Prove that n does not divide $a_k\,(a_1 - 1)$.*

Sol. Let us say for the sake of contradiction that $n \mid a_k\,(a_1 - 1)$, then

$$n \mid a_1(a_2-1) \iff a_1a_2 \equiv a_1 \pmod{n} \tag{3.1}$$
$$n \mid a_2(a_3-1) \iff a_2a_3 \equiv a_2 \pmod{n} \tag{3.2}$$
$$n \mid a_3(a_4-1) \iff a_3a_4 \equiv a_3 \pmod{n} \tag{3.3}$$
$$\vdots$$
$$n \mid a_{k-1}(a_k-1) \iff a_{k-1}a_k \equiv a_{k-1} \pmod{n} \tag{3.4}$$
$$n \mid a_k(a_1-1) \iff a_ka_1 \equiv a_k \pmod{n} \tag{3.5}$$

Note that, we should not cancel $a_i's$ from the modular equations because by the last property the (mod n) will change to (mod $\frac{n}{\mathrm{GCD}(a_i,n)}$).

Please Turn Over...

Solution Continued...

Let us start from the congruence equation in 3.1. Substitute Equation 3.2 in the Equation 3.1, to get $a_1a_2a_3 \equiv a_1 \pmod{n}$. Now substitute Equation 3.3 in the above Equation to get $a_1a_2a_3a_4 \equiv a_1$. If we continue to substitute all the equations till the Equation 3.4, we get that $a_1a_2a_3 \cdots a_k \equiv a_1 \pmod{n}$.

Similarly, if we start from the congruence equation in 3.2 and substitute Equation 3.3, we get $a_2a_3a_4 \equiv a_2 \pmod{n}$. Upon continuing the substitution till the Equation 3.5, we get $a_2a_3 \cdots a_ka_1 \equiv a_2 \pmod{n}$.

From the above two paragraphs, we conclude that $a_1 \equiv a_1a_2a_3 \cdots a_k \equiv a_2 \pmod{n} \Rightarrow a_1 \equiv a_2 \pmod{n}$. But this is a contradiction, because a_1, a_2 are distinct elements of $\{1, 2, \ldots, n\}$ and hence cannot be congruent to each other as they should leave distinct remainders when divided by n.

Question 3.2. *Find the remainder obtained upon dividing the sum*

$$1! + 2! + 3! + 4! + \cdots + 99! + 100!$$

by 12.

Question 3.3. *Prove that* 41 *divides* $2^{20} - 1$.
[*Hint :* $2^{10} \equiv -1 \pmod{41}$]

Question 3.4. *Prove that* $43 \mid 6^{n+2} + 7^{2n+1}$.
Sol. $7^2 \equiv 6 \pmod{43} \implies 7^{2n} \equiv 6^n \pmod{43}$ and $-7 \equiv 6^2 \pmod{43}$. Multiplying the above two equations, we get $-7^{2n+1} \equiv 6^{n+2} \pmod{43}$
$\implies 43 \mid 6^{n+2} + 7^{2n+1}$

Question 3.5. *Prove that* $1^n + 2^n + \cdots + (n-1)^n$ *is divisible by* n *for odd* n.

Question 3.6. *Prove that* 10^{3n+1} *cannot be represented as a sum of the cubes of two integers.*
[*Hint : Go* (mod 7)]

Remark. Work out to find that the remainders of squares (mod 3) ; cubes (mod 7) ; 5^{th} power (mod 11) ; 6^{th} power (mod 13) ; etc, can only be 0 (or) ± 1! Think about the reason behind it.