RAM Math Circle - Chennai

Synopsis for September 7 2025

This session was a review of modular arithmetic for the new students who have joined our math circle.

Start by sorting integers based on the remainder obtained after division by a fixed number as follows:

1. Fix a number, say $n = 3$. What remainders are possible when one divides a number by 3? **Observation: When dividing by 3, there are 3 possible remainders, namely $0, 1$, and 2.**

2. Repeat above exercise for $n = 4, 5, 6$ etc.

3. Generalise to other numbers: When dividing by n, there are n possible remainders, namely $0, 1, 2, \ldots, (n - 1)$.

4. Imagine there are n baskets labelled $0, 1, 2, \ldots, (n - 1)$. Pick any integer, divide it by n and see what remainder is obtained. Then imagine dropping it in the basket labelled by that remainder.

Terminology: We will say that two numbers are *congruent modulo n* if they get dropped into the same basket.

Examples:

1. $5 \equiv 3 (\text{mod } 2)$

2. $12 \equiv 7 (\text{mod } 5)$

3. $8 \equiv 15 (\text{mod } 7)$

4. $15 \equiv 27 (\text{mod } 3)$

Now that we have some idea about this sorting, let us introduce the mathematical language used to express this idea and work with it.

Definition: Let a, b and n be integers. We say that *a is congruent to b modulo n* if n divides $(b - a)$, that is $(b - a)$ is a multiple of n.

To avoid writing so many words all the time, we use

Notation: $a \equiv b(\textbf{mod } n)$ to mean *a is congruent to b modulo n*.
We can quickly check how this applies to the earlier examples -

---

Examples:

1. $5 \equiv 3 (\text{mod } 2)$ since 2 divides $(5 - 3)$

2. $12 \equiv 7 (\text{mod } 5)$ since 5 divides $(12 - 7)$

3. $8 \equiv 15 (\text{mod } 7)$ since 7 divides $(15 - 8)$

4. $15 \equiv 27 (\text{mod } 3)$ since 3 divides $(27 - 15)$

It is not too difficult to see why this definition works, that is **why a and b belong to the same basket (modulo n) if n divides $(b-a)$**. Here is a proof:

Recall the *division algorithm*: given any two integers m and n, we can find (quotient) q and (remainder) r such that

$$m = nq + r$$

and the remainder lies between 0 and $(n-1)$ (that is, $0 \leq r < n$.)

Applying the division algorithm to the pairs a, n and b, n tells us that we can find numbers q_1, q_2 and r_1, r_2 satisfying

$$a = nq_1 + r_1, 0 \leq r_1 < n$$

$$b = nq_2 + r_2, 0 \leq r_1 < n.$$

Then

$$\begin{aligned} b - a &= nq_2 + r_2 - (nq_1 + r_1) \\ &= n(q_2 - q_1) + r_2 - r_1 \end{aligned}$$

If a and b leave the same remainder when divided by n, then $r_1 = r_2$, so $r_2 - r_1 = 0$, which gives $b - a = n(q_2 - q_1)$. So $(b-a)$ is a multiple of n.

Conversely, if n divides $(b-a)$, then $r_2 - r_1$ must be zero, i.e. $r_1 = r_2$ which means a and b belong to the same basket (labelled by r_1 or r_2).