IMSc - RAM Math Circle - Chennai

Synopsis for August 30, 2026

In this session, we gathered the conclusions from our work in the earlier sessions:

- walks on polygons
- shift ciphers on the English alphabet
- figuring out the day of the week

In particular we recorded this observation:

Situation	**What do we want to figure out?**	**What matters?**
Walks on a $n-$gon with step size k	What values of k result in a complete walk?	g.c.d.(k, n)
	Which different step sizes result in the same walk?	Remainder after division by n
Shift ciphers	Which keys result in the same encryption/decryption	Remainder after division by 26
Day of the week	Given a reference date and the corresponding weekday, how do we predict the weekday for any other date?	Remainder after division by 7

We use the observations in all these situations to introduce **modular arithmetic.**

We 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 $(27-15)$
