September 15 2024

RAM Math Circle - Chennai

Sessions 2 and 3

Session format:

- 60 minutes: Introduction to modular arithmetic
- 30 minutes: Geometry with paper folding

---

1 Shift ciphers continued

We made the following observations about the working of the shift cipher (on the English alphabet):

1. Shifting by t is same as shifting by $t - 26$ or $-(26 - t)$
2. Shifting by t_1 and then shifting again by t_2 is same as shifting by $t_1 + t_2$. So *layered shifting* or applying multiple shifts provides no advantage.

The language of modular arithmetic provides a better way to express these ideas.

2 Modular arithmetic

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

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

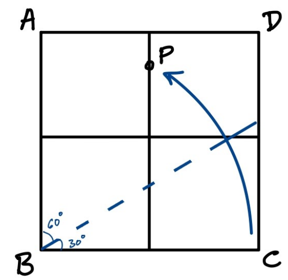
If a and b leave the same remainder when divided by n, then $r_1 = r_2$, so $r_2 - r_1 = 0$, which gives $b - a = n(q_2 - q_1)$. So $(b-a)$ is a multiple of n.

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).

3 Folding 30° and 60° angles in a square

First we will see how to fold these angles at a corner of the square. Notice that you already have a 90° at the corner, and folding a square along any one of its diagonal gives a 45° angle.

Try the construction shown in the following image:



4 Food for thought

1. For each of the following statements, choose the correct option, and state the reason for your choice:

   (a) $18 \equiv 28(\text{mod } 12) \cdots\cdots$ True/False. This is because 12 does not divide $(28 - 18) = 10$.

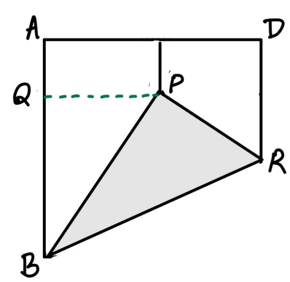
   (b) $12 \equiv 7(\text{mod } 5) \cdots\cdots$ True/False. This is because ____________________.

   (c) $8 \equiv 15(\text{mod } 7) \cdots\cdots$ True/False. This is because ____________________.

   (d) $15 \equiv 27(\text{mod } 3) \cdots\cdots$ True/False. This is because ____________________.

2. Prove that the angle obtained using the construction shown earlier is a 30° angle. You can use the following steps as guideline for your proof:

   - Notice that after making the fold the paper looks as follows:

   You want to show that angle PBR equals 30°.

   - Drop a perpendicular PQ to segment AB. Do you see a pair of similar triangles that you could use to prove the required statement?