IIIT Delhi - RAM Maths Circle
Session 14

(Organized by the Department of Mathematics, IIIT Delhi)

IIIT-Delhi December 21st, 2025

Review of modular arithmetic

Let us first recall the modular arithmetic. Look at your clock. The numbers are from $1, 2, \ldots, 12$. We have two formatted time, one is after 12 it is continued until 23 and another one restarted from 1. It suggests that 13 is "same" as 1, 14 is "same" as 2 and so on. We can think of this as when we divide any number by 12, then by the division algorithm we can only have twelve possibility for the remainder, that is, $0, 1, 2, \ldots, 11$. If you've been paying attention, you may have noticed that all that's happening here is that we're taking the remainder from some time on the 24-hour clock divided by 12. This idea can be generalized for any integers.

Mathematically, we write it as

$$a \equiv b \pmod{n},$$

which is read as a *is congruent to* b *mod* n. This means

$$n|(a-b), \quad n \text{ divides } (a-b).$$

Equivalently, $a - b = nk$ for some integer k which implies, $a = b + nk$ for some integer k. For example,

$$\begin{aligned} &23 \equiv 2 \pmod{7} && \text{as } 7|(23-2) \\ &23 \equiv -5 \pmod{7} && \text{as } 7|(23-(-5)) \\ &23 \equiv 9 \pmod{7} && \text{as } 7|(23-9). \end{aligned}$$

Note that -5 and 9 are not remainders when we divide 23 by 7.

Some properties

1. **Addition:** If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then

$$\begin{aligned} &a + q \equiv b + q \pmod{n} && \text{for any } q \in \mathbb{Z}; \\ &a + c \equiv b + d \pmod{n}. \end{aligned}$$

2. **Multiplication:** If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$, then

$$aq \equiv bq \pmod{n} \quad \text{for any } q \in \mathbb{Z};$$
$$ac \equiv bd \pmod{n}.$$

Warm-up problems

Problem 1: Prove the following properties:

(i) If $a \equiv b \pmod{n}$, then $b \equiv a \pmod{n}$.

(ii) $a \equiv a \pmod{n}$.

(iii) If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$.

Problem 2: Solve the following:

(i) Find the unit digit of 4^{2025}.

(ii) What is the remainder when 25^{2025} is divided by 6.

(iii) Find the unit digit of 2025^{2025}.

(iv) Find the last two digits of 504^{4044}.

Problem 3: What are the last two digits of the product of 34^{2021} and 37^{2022} divided by 35.

Intermediate problems

Problem 1: Prove that no number in the following sequence can be a perfect square:

$$11, 111, 1111, \ldots.$$

Problem 2: What is the remainder when $(1! + 2! + 3! + 4! + 5! + 6! + \cdots +)$ is divided by 9?

Problem 3: What is the remainder when $2^n + 6 \cdot 9^n$ is divided by 7 for any positive integer n?

Problem 3: Which digits must we substitute for a and b in $30a0b03$ so that the resulting integer is divisible by 13?

Challenging problems

Problem 1: According to *Wilson's theorem*, if p is a prime number, then

$$(p-1)! \equiv -1 \pmod{p},$$

where $n! = n \times (n-1) \times \ldots 1$. Let $n > 3$ be a positive integer. Prove that n is a prime number if and only if there exists a positive integer α such that $n! = n(n-1)(\alpha n + 1)$.

Problem 2: Let $a < b$ be two positive integers. Prove that in each set of b consecutive positive integers there are two numbers whose product is divisible by ab.