IIIT Delhi - RAM Maths Circle
Session 13

(Organized by the Department of Mathematics, IIIT Delhi)

IIIT-Delhi December 14th, 2025

Review of some number theory concepts

(a) **Well-ordering principle**. Any non-empty subset of natural numbers have a least element.

(b) **Division algorithm.** For any integers a, b, there exist unique integers q (the quotient) and r (the remainder) such that

$$a = bq + r, \quad 0 \leq r < b.$$

(c) Using the division algorithm, we can find the gcd of two nonzero numbers (Euclidean Algorithm).

Problem 1. In this problem, we want to prove the division algorithm using the well-ordering principle. We want to show the existence of quotient and remainder, so for that we consider a set

$$\mathcal{S} = \{a - bq : q \in \mathbb{Z} \text{ and } a - bq \geq 0\}.$$

(i) Show that the set $\mathcal{S}$ is non-empty.

(ii) Use well-ordering principle to get a minimum of the set $\mathcal{S}$, say r. This implies there exists $q \in \mathbb{Z}$ such that $r = a - bq$. Show that $0 \leq r < b$.

(iii) Finally, show that the quotient and remainder are unique.

Please go on to the next page. . .

Division algorithm for polynomials

Similar to the division algorithm for integers, we have a division algorithm for polynomials with rational coefficients. If $p(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ is a polynomial with rational coefficient, that means $a_0, a_1, \ldots, a_n$ are rational numbers. We write $p(x) \in \mathbb{Q}[x]$. If $a_n \neq 0$, then n is the degree of the polynomial $p(x)$. The division algorithm for polynomials is as follows: If $a(x)$ and $b(x)$ are two polynomials with rational coefficients, then there exist unique quotient and remainder polynomials $q(x), r(x) \in \mathbb{Q}[x]$ such that

$$a(x) = b(x)q(x) + r(x), \quad \deg(r) < \deg(b) \text{ or } r(x) = 0.$$

Problem 2. Calculate $q(x)$ and $r(x)$ for the polynomials $a(x) = x^4 + 3x^3 + 10$ and $b(x) = x^2 - x$.

Problem 3. What is the sum of all integers n such that n^2+2n+2 divides $n^3+4n^2+4n-14$?

Problem 4. What is the largest positive integer n such that $n^3 + 100$ is divisible by $n + 10$?

Homework-1. The numbers in the sequence $101, 104, 109, 116, \ldots,$ are of the form $a_n = 100 + n^2$, where $n = 1, 2, 3, \ldots$. For each n, let d_n be the greatest common divisor of a_n and a_{n+1}. Find the maximum value of d_n as n ranges through the positive integers.

Homework-2. Let m, n be relatively prime positive integers. Calculate $gcd(5^m + 7^m, 5^n + 7^n)$.

Bezout's Identity

For $a, b \in \mathbb{N}$, there exist $x, y \in \mathbb{Z}$ such that $ax + by = gcd(a, b)$.

Problem 5. Express 5 as a linear combination of 45 and 65.

Problem 6. Show that the quotient $\frac{21n+4}{14n+3}$ is irreducible for every natural number n. That is, the $\gcd(21n + 4, 14n + 3) = 1$ for any natural number n.