Maths Circle India: Module 8, Session 3

Organized by Indian Statistical Institute

Session Date: 17th February, 2023

1 Greatest Common Divisor

Suppose a and b are two positive integers. A positive integer d is called the greatest common divisor (gcd) (also known as highest common factor or hcf) of a and b if

- d divides both a and b;
- if a positive integer c divides both a and b, then c divides d.

(Here m divides n means n is divisible by m.)

(i) Assume that $a > b$. We can find integers q_0, r_0 such that $a = q_0 b + r_0$, where $q_0 \geq 1$ and $0 \leq r_0 < b$. If $r_0 = 0$, we then find integers q_1, r_1 such that $b = q_1 r_0 + r_1$, where $q_1 \geq 1$ and $0 \leq r_1 < r_0$. Again if $r_1 = 0$ we divide r_0 by r_1 and get remainder r_2, and so on. This process eventually terminates (Why?), and we get $r_{n-2} = q_n r_{n-1} + r_n$, and finally $r_{n-1} = q_{n+1} r_n$.

- Show that r_n divides both a and b.
- If c is a common divisor of a and b, then show that c divides r_n.

In particular, according to the definition of gcd given above, r_n is the gcd of a and b. This will prove that the Euclidean algorithm of finding gcd actually works.

(ii) Let $a > b$. Prove that the gcd of a and b is the same as the gcd of $a - b$ and b.