Maths Circle India: Module 8, Session 4

Organized by Indian Statistical Institute

Session Date: 10th March, 2023

2 More About GCD

You already know how to define and compute the gcd of two positive integers. We have discussed these in details in the previous session. What will be the gcd of a finite or an infinite collection A of positive integers? How should one define it?

Definition. Let A be any (finite or infinte) set of positive integers. A positive integer d is called the greatest common divisor (gcd) of A if

1. d divides every element of A; and,
2. if c is a positive integer such that c divides every element of A, then c divides d.

In this case, we write $d = \gcd(A)$.

- Why should $\gcd(A)$ exist for any set A of positive integers?
- First consider the case $A = \{a_1, a_2, a_3\}$. Show that

$$\gcd(A) \left(= \gcd(a_1, a_2, a_3)\right) = \gcd\left(\gcd(a_1, a_2), a_3\right).$$

- More generally, if $A = \{a_1, a_2, \ldots, a_n\}$, then show that

$$\gcd(A) \left(= \gcd(a_1, a_2, \ldots, a_n)\right) = \gcd\left(\gcd(a_1, a_2, \ldots, a_{n-1}), a_n\right).$$

Using this, show that there are integers $m_1, m_2, \ldots, m_n$ such that

$$\gcd(a_1, a_2, \ldots, a_n) = m_1 a_1 + m_2 a_2 + \cdots m_n a_n.$$

Calculating gcd of an infinite set is not that scary actually. In fact, it is the same as that of a finite subset.

- For any set A of positive integers, show that there exists a finite subset B of A satisfying $\gcd(B) = \gcd(A)$.

Now, consider the following problem.

- Take a subset A of positive integers, which
  1. has $\gcd(A) = 1$, and
  2. is closed under addition, that is, if $a, b \in A$, then $a + b \in A$.

Show that A has two consecutive integers, namely, there exists $m \in A$, such that $m + 1 \in A$ as well.

[Hint: Consider the least gap k between two consecutive elements of A. It means there exists $m, m + k \in A$. We shall show that $k = 1$. Suppose $k > 1$. First show that there exists $n \in A$ such that k does not divide n. Then write $n = qk + r$, where q, r are nonnegative integers with $0 < r < k$. Show that $(q+1)(m+k), n+(q+1)m \in A$ and this is a contradiction (why?).]

Further show that eventually all numbers are in A, namely there exists $n_0 \in A$, such that for all $k \geq n_0$, we have $k \in A$.

[Hint: We already prove there exists $m, m + 1 \in A$. Define $n_0 = m^2$. Take $l \geq n_0 = m^2$. Writing $l - m^2 = qm + r$ for nonnegative integers q, r with $0 \leq r < m$, show that $l \in A$. This will show that A contains all the positive integets starting from n_0.]