Notes

Santhosh Kumaran

Contents

Chapter 1

Real Numbers

- **Theorem 1.1** (Euclid's Division Lemma). *Given two positive integers a and b, there exist unique whole numbers satisfying $a = bq + r, 0 \leq r < b$.*

- *Euclid's division algorithm*: In order to compute the HCF of two positive integers, say a and b, with $a > b$, we take the following steps:

  - Apply Euclid's division algorithm to a and b. and obtain whole numbers q_1 and r_1 such that $a = bq_1 + r_1, 0 \leq r_1 < b$.
  - If $r_1 = 0$, b is the HCF of a and b.
  - If $r_1 \neq 0$, apply Euclid's division lemma to b and r_1 and obtain whole numbers q_2 and r_2 such that $b = r_1 q_2 + r_2$.
  - If $r_2 = 0$, then r_1 is the HCF of a and b.
  - If $r_2 \neq 0$, then apply Euclid's division lemma to r_1 and r_2 and continue the above process until the remainder r_n is zero. The divisor at this stage, i.e. r_{n-1}, or the non-zero remainder at the previous stage, is the HCF of a and b.

- **Theorem 1.2** (The Fundamental Theorem of Arithmetic). *Every composite number can be expressed as a product of primes, and this factorisation is unique apart from the order in which the prime factors occur.*

- Every composite number can be uniquely expressed as a product of powers of primes in ascending or descending order.

- The HCF of two or more numbers is the product of the smallest powers of each of the numbers' common prime factors.

- The LCM of two or more numbers is the product of the greatest powers of each of the numbers' prime factors.

- For any two positive integers a and b, $ab = \text{HCF}(a, b) \times \text{LCM}(a, b)$

- **Theorem 1.3.** *Let a be a positive integer and p be a prime number. If p divides a^2, then p divides a.*

- If p is a prime number, then $\sqrt{p}$ is an irrational number.

  Proof. Assume, to the contrary, that $\sqrt{p}$ is a rational number and express it thus:

  $$\sqrt{p} = \frac{a}{b}$$

  where a and b are co-prime integers and $q \neq 0$. Next, isolate a and square the equation:

  $$b\sqrt{p} = a \tag{1.1}$$
  $$pb^2 = a^2 \tag{1.2}$$

  Since p divides a^2, p divides a (as per Theorem 1.3). Therefore,

  $$a = pc$$

  for some integer c. Substitute for a in Equation 1.2:

  $$pb^2 = (pc)^2$$
  $$pb^2 = p^2c^2$$
  $$b^2 = pc^2$$

  Since p divides b^2, p divides b (as per Theorem 1.3). p is a common factor of a and b This contradicts the fact that a and b are co-prime. Our assumption that $\sqrt{p}$ is rational is incorrect. Hence, $\sqrt{p}$ is irrational. QED