

A. Introduction

-- In this chapter, we will discuss two very important properties of positive integers, namely the Euclid's division algorithm and the Fundamental Theorem of Arithmetic.

B. Euclid's Division Lemma

Stated simply, it says any positive integer a can be divided by another positive integer b in such a way that it leaves a remainder r that is smaller than b .

Theorem: (Euclid's Division Lemma) : Given positive integers a and b , there exist unique integers q and r satisfying $a = bq + r$, $0 \leq r < b$.

-- Euclid's division algorithm is a technique to compute the Highest Common Factor (HCF) of two given positive integers. To obtain the HCF of two positive integers, say c and d , with $c > d$, follow the steps below:

Step1: Apply Euclid's division lemma, to c and d . So, we find whole numbers, q, r such that $c = dq + r$, $0 \leq r < d$.

Step2: If $r = 0$, d is the HCF of c and d . If $r \neq 0$, apply the division lemma to d and r .

Step3: Continue the process till the remainder is zero. The divisor at this stage will be the required HCF.

-- An algorithm is a series of well-defined steps which gives a procedure for solving a type of problem. A lemma is a proven statement used for proving another statement.

Suppose we need to find HCF of the integers 455 and 42. We start with the larger integer, that is, 455. Then we use Euclid's lemma to get $455 = 42 \times 10 + 35$

Now consider the divisor 42 and the remainder 35, and apply the division lemma to get $42 = 35 \times 1 + 7$

Now consider the divisor 35 and the remainder 7, and apply the division lemma to get $35 = 7 \times 5 + 0$

Notice that the remainder has become zero, and we cannot proceed any further. We claim that the HCF of 455 and 42 is the divisor at this stage, i.e., 7.

Example: Show that any positive odd integer is of the form $4q + 1$ or $4q + 3$, where q is some integer.

-- Let us start with taking a , where a is a positive odd integer. We apply the division algorithm with a and $b = 4$. Since $0 < r < 4$, the possible remainders are 0, 1, 2 and 3. That is, a can be $4q$, or $4q + 1$, or $4q + 2$, or $4q + 3$, where q is the quotient.

However, since a is odd, a cannot be $4q$ or $4q + 2$ (since they are both divisible by 2). Therefore, any odd integer is of the form $4q + 1$ or $4q + 3$.

C. The Fundamental Theorem of Arithmetic

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

Example: Consider the numbers $4n$, where n is a natural number. Check whether there is any value of n for which $4n$ ends with the digit zero.

-- If the number $4n$, for any n , were to end with the digit zero, then it would be divisible by 5. That is, the prime factorisation of $4n$ would contain the prime 5. This is not possible because $4n = (2)2n$; so the only prime in the factorisation of $4n$ is 2.

So, the uniqueness of the Fundamental Theorem of Arithmetic guarantees that there are no other primes in the factorisation of $4n$. So, there is no natural number n for which $4n$ ends with the digit zero.

A. Revisiting Irrational numbers

Irrational Numbers: Any numbers that cannot be written in form a/b , where a and b are integers and $b \neq 0$.

E.g. $\sqrt{5}$, $\sqrt{3}$, $\sqrt{10}$, π (called Pi).

Theorem: Let p be a prime number. If p divides a^2 , then p divides a , where a is a positive integer.

Theorem: $\sqrt{2}$ is irrational.

Example: Show that $5 - \sqrt{3}$ is irrational.

-- Let us assume, to the contrary, that $5 - \sqrt{3}$ is rational. That is, we can find coprime a and b ($b \neq 0$) such that $5 - \sqrt{3} = \frac{a}{b}$. Therefore, $5 - \frac{a}{b} = \sqrt{3}$. So, $\sqrt{3} = 5 - \frac{a}{b} = \frac{5b-a}{b}$. Since a and b are integers, we get $5 - \frac{a}{b}$ is rational, and so $\sqrt{3}$ is rational. But this contradicts the fact that $\sqrt{3}$ is irrational. Assumption is incorrect that $5 - \sqrt{3}$ is rational. So, we conclude that $5 - \sqrt{3}$ is irrational.

B. Revisiting Rational numbers and their Decimal Expansions

Rational Numbers: Any number that can be written in form a/b , where a and b are integers and $b \neq 0$.

E.g. 7, 8, $5/10$, $-3/4$, $31/12$

Terminating Decimals (Rational Numbers):

E.g. $1/2 = 0.5$, $1/4 = 0.25$

Non-terminating and Recurring Decimals (Rational):

E.g. $1/3 = 0.333... = 0.\overline{3}$, $1/6 = 1.6666... = 1.\overline{6}$,

$1/7 = 0.142857142857.. = 0.\overline{142857}$

Non-terminating Non-recurring Decimals (Irrational):

E.g. $\sqrt{3} = 1.4142.....$, $\pi = 3.14159.....$

Theorem: Let x be a rational number whose decimal expansion terminates. Then x can be expressed in the form $\frac{p}{q}$, where p and q are coprime, and the prime factorisation of q is of the form $2^n 5^m$, where n, m are non-negative integers.

Theorem: Let $x = \frac{p}{q}$ be a rational number, such that the prime factorisation of q is of the form $2^n 5^m$, where n, m are non-negative integers. Then x has a decimal expansion which terminates.

Theorem: Let $x = \frac{p}{q}$, where p and q are co-primes, be a rational number, such that the prime factorisation of q is not of the form $2^n 5^m$, where n, m are non-negative integers. Then, x has a decimal expansion which is non-terminating repeating (recurring).