

Lesson Summary

1. Prime Factorization

- The process of dissecting a composite number into its prime factors is known as prime factorization. This idea is crucial to number theory and has numerous uses in computer science, cryptography, and other disciplines. According to the fundamental theorem of arithmetic, any integer larger than one is either a prime number or the product of prime numbers.

Prime factorization is the practice of continuously dividing a number by its smallest prime factor until the quotient equals 1. The original number is then formed by multiplying all of the prime factors that were obtained throughout this step.

✓ Euclidean Algorithm

- A technique for determining the greatest common divisor (GCD) of two numbers is the Euclidean algorithm. The greatest positive integer that divides both numbers without leaving a remainder is the GCD of two integers. The algorithm is based on the observation that the GCD of a and b is the same as the GCD of b and the remainder of a divided by b if a and b are two positive integers with $a > b$ and $a \geq b$.

Until the smaller number equals zero, the algorithm keeps going by continuously substituting the bigger number with the remaining amount after dividing the larger number by the smaller number. The GCD of the initial two numbers is the final non-zero remainder.

2. Base Conversion

- The process of translating a number from one number base to another is called base conversion. The number of distinct digits (including zero) used to represent numbers in a positional numeral system is called the number base, sometimes referred to as the radix.

A number can be converted from one base to another by splitting it into its component parts, multiplying each part by the relevant base power, and then adding the results. Repetitive division or multiplication can be used for this procedure, depending on whether you're converting from a lower base to a higher base or the other way around.

3. Modular arithmetic

- In the integer arithmetic system known as modular arithmetic, numbers "wrap around" when they reach a particular value known as the modulus. Because it mimics the operation of a clock, it is often referred to as clock arithmetic.

Numerous domains, including computer science, cryptography, number theory, and others where computations entail cyclical or recurring patterns, use modular arithmetic. Additionally, it's essential for comprehending ideas like modular exponentiation and congruence.