My Reflection on week 1 Class on Discrete mathematics

Prime factorization and the Euclidean algorithm

The exercise starts with some definitions that are basic in nature and introduce the idea of factors and divisibility in relation to the division of integers. Integers classified as prime numbers can only be divided by one and themselves, whereas composite numbers can also be divided by factors ither than one and themselves. As per the fundamental theorem of arithmetic any positive integer larger than 1 can be expressed uniquely as a product of prime numbers. Prime factorization of the process of expressing a composite number as the product of its prime factor. The activity also covers the use of prime factorizations to find the LCM (Lowest Common Multiple) and GCD (Greatest Common Divisor). In order to make the process of determining the GCD of two numbers easier without having to explicitly compute their prime factorization, the Euclidean algorithm is presented.

Few uses of this are that we can use it for understanding numbers, to represent something uniquely, such as in cryptography, can be used to do calculations efficiently, helps for problem solving and its versatility where it can be applied in wide range of application.

Base conversion

The tasks present the idea of base systems, highlighting the fact that base 10 is the numeral system we are most familiar with, with the digits denoting increasing powers of 10. Examples are provided to show how various base systems, including base 5, base 2(binary), and base 8, are represented. There are real-world examples of base systems in action, including the measurement of angles in a circle, the division of a year into months, and the division of days in to hours. There are two ways to explain base 10 conversions to other base systems. In method, the number is divided by the base’s powers one after the other, and in Method 2, the base is divided and the remainders are noted.

Its main uses are in computer science. There are real-world applications as mentioned above. Practicing base conversion will help us become strong in cognitive skills and logical thinking.

Modular arithmetic

In modular arithmetic, the remainder of an integer divided by another integer is expressed. The notation "a≡b(modm)" means that when a and b are divided by m, the remainders are the same. Modular arithmetic for both positive and negative integers is demonstrated through examples.

In modular arithmetic, addition and multiplication are introduced. Rules for modular arithmetic are demonstrated, which state that if b≡d and a≡c, then (a+b) ≡ (c+d) and (a×b) ≡ (c×d) are valid. The same rules hold for big numbers as well. The validity of the rule is demonstrated by logical proof. In modular arithmetic, the powers of two are investigated and a pattern is found. We go over general guidelines for computing powers in modular arithmetic. The computation of 29307 (mod 67) is guided by an exercise that also includes the knowledge that 293 (mod 67) = 1293 (mod67) = 1.

It is mainly used in cryptographic applications, efficient computation with large numbers, understanding periodic patterns, Real-World time keeping and many more.

References

Prime factorization and the Euclidean algorithm

1. Wikipedia contributors. (2023b, November 25). *Euclidean algorithm*. Wikipedia. <https://en.wikipedia.org/wiki/Euclidean_algorithm#:~:text=It%20is%20used%20for%20reducing,by%20factoring%20large%20composite%20numbers>.

Base conversion

1. *Base Conversion | System Design Library*. (n.d.). <https://leetdesign.com/library/base_conversion>

Modular arithmetic

1. *Modular arithmetic*. (2021, January 22). Let’s Talk Science. <https://letstalkscience.ca/educational-resources/backgrounders/modular-arithmetic#:~:text=Modular%20arithmetic%20has%20many%20applications,involve%20long%20strings%20of%20numbers>.