ZK Core Concepts:

Modular Arithmetics:
The modulo is the remainder after x/y that is what remains after y into x.

Known Patterns of Modulo:
If x is a multiple of y: x % y = 0

If x is one more than a multiple of y: x % y = 1

If x is one less than a multiple of y: x % y = y - 1

If y is greater than x: x % y = x

If x is 0: x % y = 0 (for any value of y)

Commutative Groups:

A commutative group (G, *) consists of:

1. **Closure Property:** For all elements a, b in G, the result of the operation * on a and b, denoted as a * b, is also an element of G.
   - $\forall a, b \in G, a * b \in G$
2. **Associativity Property:** For all elements a, b, and c in G, the operation * is associative.
   - $\forall a, b, c \in G, (a * b) * c = a * (b * c)$
3. **Identity Element:** There exists an element e (the identity element) in G such that for all elements a in G, the operation * of a with e results in a.
   - $\exists e \in G$ such that $\forall a \in G, a * e = a$ and $e * a = a$
4. **Inverse Element:** For each element a in G, there exists an element a^(-1) (the inverse of a) in G such that the operation * of a with its inverse a^(-1) results in the identity element e.
   - $\forall a \in G, \exists a^{(-1)} \in G$ such that $a * a^{(-1)} = e$ and $a^{(-1)} * a = e$
5. **Commutativity (Abelian Property):** For all elements a, b in G, the operation * is commutative, meaning that the order of elements in the operation does not affect the result.
   - $\forall a, b \in G, a * b = b * a$

These five properties define a commutative group (G, *) in abstract algebra, where the binary operation * is both associative and commutative within the given set G

Generators in Cyclic Groups:

A cyclic group is a specific type of group in abstract algebra that can be defined mathematically as follows:

A group G is said to be cyclic if there exists an element a in G such that, for every element g in G, there exists an integer n such that:

$g = a^n$

In this definition:

1. "G" is the group under consideration.
2. "a" is an element of the group G, called the generator.
3. "n" is an integer, and a^n represents the result of applying the group operation to the generator "a" repeatedly, either by multiplying "a" by itself n times if n is positive or taking the inverse of "a" and multiplying it by itself |n| times if n is negative.

In other words, a group G is cyclic if it can be generated by a single element a such that every element of the group can be expressed as a power of a.

Discrete Logarithm Problem:

Given a cyclic group G of order n, a generator g of that group, and an element h in the group G, the Discrete Logarithm Problem is to find an integer x such that:

$g^x \equiv h \pmod{n}$

In this definition:

- G is a finite cyclic group with order n. The order of a group is the number of elements it contains.
- g is an element of G, called a generator, such that every element in G can be expressed as a power of g.
- h is another element in G.
- x is the integer we want to find, and it's referred to as the discrete logarithm of h to the base g in G.
- ≡ denotes congruence modulo n, meaning that g^x and h have the same remainder when divided by n.

The problem is computationally difficult, especially when the values of n, g, and h are chosen such that it's challenging to efficiently compute x.