Homework 1

> Maths Introduction
>
> ## Some modular arithmetic
>
> 1. Working with the following set of Integers S = {0,1,2,3,4,5,6}
>
>   What is
>
>   a) 4 + 4 = 8 =1
>
>   b) 3 x 5 = 15 =1
>
>   c) what is the inverse of 3 ? 3 x 5 = 15 = 1 —> x^-1 = 5
>
> 2. For S = {0,1,2,3,4,5,6}
>
>   Can we consider 'S' and the operation '+' to be a group ?
>
> 3. What is
>
>   -13 mod 5 ? = -2 = 2
>
> 4. Polynomials
>
>   For the polynomial $x^3 - x^2 + 4x - 12$
>
>   Find a the positive root ?
>
>   What is the degree of this polynomial ? 3 degree

2) To determine whether the set S = {0, 1, 2, 3, 4, 5, 6} along with the operation "+" forms a group, we need to check if it satisfies the four fundamental properties of a group:

Closure: The operation must be closed within the set, meaning that when you combine any pair of elements from the set using the operation, the result must also be in the set. In this case, the operation "+" is closed in set S because the sum of any two elements in S results in another element in S.

Associativity: The operation must be associative, which means for any elements a, b, and c in S, the operation must satisfy (a + b) + c = a + (b + c). The addition operation in set S is indeed associative.

Identity Element: A group must contain an identity element (denoted as "e" or "0") such that for any element "a" in the set, a + e = e + a = a. In this case, the identity element is 0 because for any element "a" in set S, a + 0 = 0 + a = a.

Inverses: Every element in the set must have an inverse under the operation. For the addition operation, the inverse of an element "a" is the element "b" such that a + b = b + a = 0. In set S, the inverse of an element "a" is simply the additive inverse (-a), which, when added to "a," results in the identity element (0).

Since set S = {0, 1, 2, 3, 4, 5, 6} along with the operation "+" satisfies all four properties of a group (closure, associativity, identity element, and inverses), it can be considered a group under the addition operation.

> **Use cases**
>
> In your teams discuss any systems you have used that involved zero knowledge proofs.
>
> Have you seen any applications of zero knowledge proofs other than with a blockchain ?
>
> What is to you, the most important feature of zkp technology ?
>
> Think of some use cases of zero knowledge proofs that you would like to see developed.