Homework 1

Maths Introduction

Some modular arithmetic

1. Working with the following set of Integers S = {0,1,2,3,4,5,6} **Meaning that the prime number is 7**

   What is

   a) 4 + 4 **4+4 = 8 = 1 mod 7**

   b) 3 x 5 **3x5 = 15 = 1 mod 7**

   c) what is the inverse of 3 ? ***Applying Fermat little's theorem: Multiplicative inverse: 3^(7-2) mod 7 = 5, *Additive inverse is 4 : 3 + 4 mod 7 = 0**

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 ? **-13 mod 5 = 2**

4. Polynomials

   For the polynomial $x^3 - x^2 + 4x - 12$

   Find a the positive root ? **Solve where eq = 0, x = 2**

   What is the degree of this polynomial ? **Degree = 3**

2) (S,+s) is a group.

i. Closure
(S,+s) is close under the +s operation. Since it is Z7, for all a, b in S, a +s b mod 7 in the S.

ii. Associativity
From the closure, a +s b = (a + b) mod 7 where + operation is ordinary addition in Z.
a +s (b +s c) = (a + b) + c mod 7 (from (Z, +) is associative)
(a + b) + c mod 7 = (a +s b) +s c therefore (S,+s) is also associative.

iii. Identity Element
Is there any element a in S, so that for all b in S, a +s b is equal b.
a = 0

iv. Each element except the identity(zero), has the inverse under the addition operation.
Not elegantly :)
the inverse of 1 equals 6 since 1 +s 6 = 0
So each element has its inverse.

From i, ii, iii, and iv, (S,+s) is a group.

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.