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 mod 7 ≡ 1
   b) 3 x 5   = 15 mod 7 ≡ 1
   c) what is the inverse of 3 ? Using fermat's little theorem: 5
   3 ^ (7 - 2) ≡ 243 mod 7 ≡ 5 mod 7

2. For S = {0,1,2,3,4,5,6}
   Can we consider 'S' and the operation '+' to be a group ?   Yes

3. What is
   -13 mod 5 ?   ≡ 2 mod 5

4. Polynomials
   For the polynomial $x^3 - x^2 + 4x - 12$
   Find a the positive root ?   x = 2
   What is the degree of this polynomial ?   n = 3

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.