

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) $4 + 4$

b) 3×5

c) what is the inverse of 3 ?

2. For $S = \{0,1,2,3,4,5,6\}$

Can we consider 'S' and the operation '+' to be a group ?

3. What is

$-13 \bmod 5$?

4. Polynomials

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

Find a the positive root ?

What is the degree of this polynomial ?

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.