

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

$-13 \bmod 5$?

Use cases

In your groups, think of some use cases of zero knowledge proofs

What problems are there when using zkps in real world situations ?