ZK Bootcamp: Homework 1

Kuriakin Zeng

July 28, 2022

Math Introduction

Problem 1

Working with the following set of Integers $S = \{0, 1, 2, 3, 4, 5, 6\}$, what is:

- $4 + 4 \equiv 1 \pmod 7$
- $3 \cdot 5 \equiv 1 \pmod 7$
- By Fermat's Little Theorem, $3^{-1} \equiv 3^{7-2} \pmod 7 \equiv 5 \pmod 7$

Problem 2

$S = \{0, 1, 2, 3, 4, 5, 6\}$ and operation $+$ is a group.

Proof. For any $a, b, c \in S$

- Closure. It's easy to see that $a + b \pmod 7 \in S$
- Associativity. S is a subset of integers, thus $(a + b) + c = a + (b + c)$
- Identity. The identity element is 0 since $a + 0 = a$
- Inverse element. It's easy to see that, by FLT, $-a \equiv 5a \pmod 7$ and $-a+5a = 4a \pmod 7 \in S$

□

Problem 3

$-13 \pmod 5 \equiv 2 \pmod 5$

Use cases of zkp

- Authenticate users without exchanging secret information such as passwords
- Allow one to prove that they satisfy a requirement without revealing the data itself. For example, proving that one's income is in admissable range for a loan
- Allow voters to vote anonymously without compromising the legitimacy of the votes

However, zkp has a few challenges.

- As demonstrated by the ball-picking example, the probability of the prover lying decreases with each iteration but ZKP's don't guarantee 100% that the prover isn't lying
- zkps require many interactions between the verifier and the prover in interactive ZKP's or require a great deal of computations in non-interactive ZKP's. They may not be suitable for slow or mobile devices.