# Answers for Homework 1

Working with the following set of Integers
S = {0,1,2,3,4,5,6}

1. a) 4 + 4
   = 1 mod 7
   b) 3 x 5
   = 1 mod 7

c) what is the inverse of 3 ?

```
Using
$a^{-1} ≡ a^{p-2} (mod p)$
= 3 ^ (7-2) = 3 ^ 5 = 243
= 5 mod 7
```

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

- yes it follows all of the group proprties

3. -13 mod 5
   = 2 mod 5.

## Use cases

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

- The problems often involve trusting centalised data sources for provision of public or private inputs to the proofs