Homework 2

1. Group / field theory
   Take the set of bits `B = {0,1}` and the operation `⊕` with the following rules:

   ```
   `0 ⊕ 0 = 0`
   `0 ⊕ 1 = 1`
   `1 ⊕ 0 = 1`
   `1 ⊕ 1 = 0`
   ```

Does the set B and the operation `⊕` satisfy the group properties ?

2. Modular arithmetic - you just need to find examples, you don't need to prove anything.
   1. Is it true that all odd squares are ≡ 1 (mod 8) ?
   2. what about even squares (mod 8) ?
3. Try out the vanity bitcoin address example at asecurity or the Ethereum version
4. What do you understand by
   1. O(n)
   2. O(1)
   3. O(log n)
5. Which of those is best when describing a proof size