Homework 4

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. Cyclic Groups

   1. Take the elements {1,2,3,4,5,6,7,8,9,10,11,12} as our set (it may help to think of a clock here)
   2. Is this group finite ?
   3. Is this group cyclic ?
   4. Is 1 a generator for this group ?
   5. Is 2 a generator for this group ?

3. Modular arithmetic - you just need to find examples, you don't need to prove anything.

   1. Find some quadratic residues mod 2
   2. Is it true that all odd squares are ≡ 1 (mod 8) ?
   3. what about even squares (mod 8) ?

4. Try out the vanity bitcoin address example at asecurity or the Ethereum version