

## Homework 2

### Homework Maths 2

1. Modular arithmetic - you just need to find examples, you don't need to prove anything.
  1. Is it true that all odd squares are  $\equiv 1 \pmod{8}$  ?
  2. what about even squares  $\pmod{8}$  ?
2. Try out the vanity bitcoin address example at [asecurity](#) or the Ethereum [version](#)
3. What do you understand by
  1.  $O(n)$
  2.  $O(1)$
  3.  $O(\log n)$

For a proof size, which of these would you want ?