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 ≡ 1 (mod 8) ?
   2. what about even squares (mod 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 ?

(1.1) $3^2 \Rightarrow 9 \bmod 8 \Rightarrow 1 \bmod 8$
$5^2 \Rightarrow 25 \bmod 8 \equiv 1 \bmod 8$
$7^2 \Rightarrow 49 \bmod 8 \equiv 1 \bmod 8$
} Yes

(1.2) $4^2 \Rightarrow 16 \bmod 8 \neq 1 \bmod 8$
$6^2 \Rightarrow 36 \bmod 8 \neq 4 \bmod 8$
} No

(2)

(3) (3.1) O(n) the worst case is linear w.r.t input size
(3.2) O(1) the time is constant, doesn't change w.r.t input size
(3.3) O(log n) the time varies according to the log of input size

O(1) works fine for proof size.