Zero Knowledge Proofs: Homework 2

Meek Msaki

February 9, 2023

Question 1

Modular arithmetic

1. Answer is True. All odd squares are $\equiv 1 \mod 8$
2. All even square are either $\equiv 0 \mod 8$ or $\equiv 4 \mod 8$.

Question 2

Generated Ethereum address ending with word **CaFe**:
Public Key: 0xb2e3d94823116e9dAAd56cD95f654a1BE6e4**CaFe**.

Question 3

1. $O(n)$ means that, as the size of our input n increases, in time complexity, the time it takes for our program to find a solution grows linearly. In Space Complexity, the size n represents the space in memory that our program needs to run the computation.
2. $O(1)$ means that, as the size of our input n increases, the time it takes for our program to find a solution remains constant.
3. $O(\log n)$ means that, as that size of our input n increases, the time it takes for our program to find a solution gradually decelerates. Our input n can grow exponentially while the times our program takes grows slowly compared to the size of our input.

For proof size, which of these do we want?

$O(\log n)$, it's advantage is that while our input grows larger the size of our proofs remain relatively small.