ZK Bootcamp: Homework 2

Kuriakin Zeng

July 28, 2022

Problem 1

Proof. $B = \{0, 1\}$ and the operation $\oplus$ is a group

- Closure. It's easy to see that from the rules that the output is $\in B$
- Associativity. $0 \oplus 1 = 1 \oplus 0 = 1$
- Identity. The identity element is 0 since for $b \in B$, $b + 0 = b$ and it's unique
- Inverse element. $0^{-1} = 0$ and $1^{-1} = 1$

□

Problem 2

- Odd squares are $\equiv 1 \pmod 8$

  Proof. Squares are produced by adding consecutive odd numbers. An odd square is produced by summing the odd number of odd numbers: the first odd square is 1, the second odd square is $1+3+5 = 9$, and the subsequent odd squares is $1+3+5+(3+4n)+(5+4n)$ where $n = \{1, 2, 3, ...\}$ It's easy to see that the first two odd squares $\equiv 1 \pmod 8$ and $1 + 3 + 5 + (3 + 4n) + (5 + 4n)$ can be rewritten as $1 + 3 + 5 + (8 + 8n)$. Since $8 + 8n \equiv 0 \pmod 8$, it must be that all odd squares $\equiv 1 \pmod 8$ □

- Even squares are $\equiv 0 \pmod 8$

  Proof. An even square is produced by summing the even number of odd numbers: the first even square is $1 + 3 = 4$, and the subsequent is $1 + 3 + (1 + 4n) + (3 + 4n)$ where $n = \{1, 2, 3, ...\}$ We can rewrite the equation as $8 + 8n$, thus it must be that even squares are $\equiv 0 \pmod 8$ □

Problem 3

We generate a random private key (n) and use a point on elliptic curve (G) [secp256k1 $\rightarrow y^2 = x^3 + 7$] to generate the public key $n \cdot G$. The hash of the public key is the Bitcoin address. Helpful resource: https://www.youtube.com/watch?v=muIv8I6v1aE

Problem 4

The three represent the worst case complexity of a function, i.e. the amount of resources required to run a function in the worst case scenario

- $O(n)$ means the complexity grows linearly with respect to the input size
- $O(1)$ means the complexity doesn't grow with respect to the input size
- $O(logn)$ means the complexity grows logarithmically with respect to the input size

Problem 5

The best case for proof size is $O(1)$