Part 1 Theoretical background of zk-SNARKs and zk-STARKS

1. **Write down two types of SNARK proofs.**
    a. Groth16
    b. Sonic

2. **Explain in 2-4 sentences why SNARK requires a trusted setup while STARK doesn't.**
    A trusted setup is required to prevent the prover from cheating by providing fake proofs. Since Snarks are short proof and fast verification based, a pre-processing phase (trusted setup) must be created beforehand. This ensures that the proof time is short (succinct). On the other hand, since Stark proofs make use of hashes, there is no need of having a trusted setup

3. **Name two more differences between SNARK and STARK proofs.**
    a. Starks require high gas to verify, since the verification takes more time than Snarks.
    b. Snarks take less-on chain storage compared to Starks proofs

Part 2 Getting started with circom and snarkjs

2.

1. **What does the circuit in HelloWorld.circom do?**
    The code in the circuit contains code that can be used to prove that two inputs a and b can be multiplied to give a given output c

2. **What is a Powers of Tau ceremony? Explain why this is important in the setup of zk-SNARK applications.**
    Powers of Tau ceremony is a multi-party computation ceremony which constructs partial zk-SNARK parameters it involves parties who contribute randomness to iteratively construct the common reference string on which zk-snarks rely on.

    It's important because it makes the multiparty computation ceremony cheaper and allowing for scale without being affected by the number of parties involved

3. **How are Phase 1 and Phase 2 trusted setup ceremonies different from each other?**

   Powers of Tau which is the first phase helps to come up with the generic setup parameters that can be used by circuits in the scheme while the second phase converts the outputs of the first phase into an NP-relation specific common reference string