Problem 1: (ZK) In class we saw Zero-Knowledge protocols for proving that a number is a quadratic residue modulo $N$ and for proving equality of discrete logarithms. Your goal is to give Zero-Knowledge protocols for the complement languages. Remember to prove soundness, completeness, and zero-knowledge.

a. Give a Zero-Knowledge protocol for the language containing all pairs $(N, x)$ where $x \in \mathbb{Z}_N$ and $x$ is not a quadratic residue in $\mathbb{Z}_N$.

b. Let $G$ be a group of prime order $q$. Give a Zero-Knowledge protocol for the language containing all tuples $(g, g^a, h, h^b)$ where $g, h \in G$ and $a \neq b \mod q$.

Problem 2: (ZKPK) Let $N = pq$ and let $e$ be a prime, $e \nmid \phi(N)$. Let $v \in \mathbb{Z}_N$ and let $s = v^{1/e} \mod N$. Consider the following protocol for proving knowledge of $s$ given $(N, e, v)$:

1. Prover picks random $r \in \mathbb{Z}_N$ and sends $t = r^e \in \mathbb{Z}_N$ to verifier.
2. Verifier picks random integer $c \in [1, B]$ and sends $c$ to prover ($B$ is some fixed value).
3. Prover computes $w = s^c \cdot r \in \mathbb{Z}_N$ and sends $w$ to verifier.
4. Verifier accepts only if $w^e = v^c \cdot t$.

a. Prove that the protocol is an honest-verifier ZKPK. Remember to prove completeness, soundness, honest-verifier zero knowledge, and to demonstrate an extractor.

b. Show that there is an efficient malicious prover (who does not know $s$) that convinces the verifier with probability at least $1/e$.

c. Does it makes sense to chose $B > e$?

Problem 3: (multi-party protocols) For $i = 1, \ldots, n$ suppose that party $i$ has input $a_i \in \mathbb{Z}_p$. Describe an $n - 1$ private protocol for computing $\sum_{i=1}^n a_i$. Prove that your protocol is $n - 1$ private (remember to build a simulator for any coalition $S$ of size $|S| < n - 1$).

Problem 4: (two party protocols) Let $p$ be a prime. Suppose user $A$ has an $x \in \mathbb{Z}_p$ and user $B$ has a $y \in \mathbb{Z}_p$. They wish to compute the following function: $f(x, y) = 0$ when $x = y$ and $f(x, y) = 1$ when $x \neq y$, without revealing any other information about $x$ or $y$. Your goal is to give an efficient solution to this problem in the honest-but-curious settings.

a. Estimate the amount of communication needed for this problem using Yao’s garbled circuits method. State your estimate asymptotically as a function of $\log_2 p$. You may assume that we use the Naor-Pinkas OT in (a subgroup) of $\mathbb{Z}_p^*$.

b. Suppose there is a third party who is willing to help. Give an efficient 3-party protocol for computing $f(x, y)$ so that nothing else is revealed to any single party (1-private). Prove 1-privacy by showing a simulator for each party’s view of the protocol (the simulator is
given \( f(x, y) \) and that party’s input).

Hint: Try having the third party pick a random hash function from \( \mathcal{H} = \{ ax + b \mid a \in \mathbb{Z}_p, b \in \mathbb{Z}_p \} \).

\( \textbf{c. Extra credit: can you suggest 1-private 2-party protocol that is more efficient than Yao’s garbled circuit method? Feel free to consult the web.} \)

\( \textbf{Problem 5: (Pallier encryption)} \) We discuss the best known additive homomorphic system.

Let \( N = pq \) and let \( G \) be the multiplicative group of integers modulo \( N^2 \), i.e. \( G = (\mathbb{Z}/N^2\mathbb{Z})^* \). Then \( G \) is a group of order \( N\varphi(N) \). Let \( H \) be the subgroup of \( G \) that contains all elements \( x \in G \) satisfying \( x = 1 \mod N \). Then \( H \) is a subgroup of order \( N \).

\( \textbf{a. Show that the discrete log problem in } H \text{ is easy. That is, show that there is an efficient algorithm that given } g, g^x \in H \text{ outputs } x \mod N. \)

\( \text{Hint: note that } g = aN + 1 \text{ for some } a \in \mathbb{Z}. \text{ Use the binomial formula on } g^x. \)

\( \textbf{b. Consider the following public-key encryption system:} \)

- \( \text{KeyGen(n): pick two } n \text{-bit primes } p, q \text{ and set } N = pq. \text{ Output the public key } N \text{ and the private key } d = \varphi(N). \)
- \( \text{Encrypt(N,m): let } g = N + 1 \in G. \text{ For a message } m \in \mathbb{Z}_N \text{ pick a random } r \in G \text{ and output the ciphertext } C = g^m r^N \in G. \)
- \( \text{Using part (a) show how to decrypt a ciphertext } C \text{ using the private key } d = \varphi(N). \)

\( \text{Hint: observe that } C^{\varphi(N)} \text{ is of order } N \text{ and therefore in } H. \)

\( \textbf{c. Show that given an encryption of } x_1 \text{ and an encryption of } x_2 \text{ one can create an encryption of } x_1 + x_2 \text{ sampled from the same the distribution as is produced by the Encrypt algorithm.} \)

\( \textbf{d. Let } T \text{ be the subgroup of } G \text{ of order } \varphi(N), \text{i.e. } T = \{ r^N \mid r \in G \}. \text{ Suppose the uniform distribution on } T \text{ is } (t, \epsilon) \text{ indistinguishable from the uniform distribution on } G. \text{ Show that the system above is } (t, \epsilon) \text{ semantically secure.} \)