Week 8 Exercises (ECE 598 DA)

Exercise (Simulator for Graph Non-Isomorphism): In the Graph Non-Isomorphism protocol, construct a simulator S that produces the verifier's view without access to the prover. Prove that the distribution of S's output is identical to the distribution of the honest verifier's view when interacting with the honest prover on *non-isomorphic* graphs.

Exercise (Completeness and Soundness of QNR Protocol): Consider the Quadratic Non-Residue protocol.

- Show that if x is a quadratic non-residue mod N, the verifier accepts with probability 1 (perfect completeness).
- Show that if x is a quadratic residue, then no matter what strategy the prover uses, the verifier's acceptance probability is at most $1/2$ (soundness).

(Hint: argue that in this case $z = y^2$ (if $c = 0$) and $z' = y^2 x$ (if $c = 1$) are *indistinguishable* distributions to the prover.)

Exercise (SZK $\subseteq$ AM $\cap$ coAM): Show how any statistical zero-knowledge proof can be transformed into an **AM** protocol (public-coin, 2-message) for the same language, and likewise give a protocol for the complement (**coAM**). Outline why this implies **SZK** $\subseteq$ **AM** $\cap$ **coAM**.