Problem Set 11

This problem set is due on Friday, April 30, by 5pm. Please submit your solution online using bcourses, as a pdf file. You can type your solution, or handwrite it. If you handwrite it, then either scan it or take a good resolution picture of each page and then collate the pictures and export them to a *single* pdf file.

Problem 1 (33/100)

In $\mathbb{Z}_{77}$ find all of the elements that are quadratic residues with only two roots (as opposed to four). Showing work/reasoning could be helpful in grading.
Why do these end up not being a problem in the quadratic residuosity scheme we've seen in class? [Hint: there are eight such elements]

Problem 2 (33/100)

Recall that we defined IP as the class of languages such that for each language L there exists a pair of algorithms (or better, interacting machines) $(\mathcal{P}, \mathcal{V})$, where the verifier $\mathcal{V}$ is polynomial in $|x|$ such that:

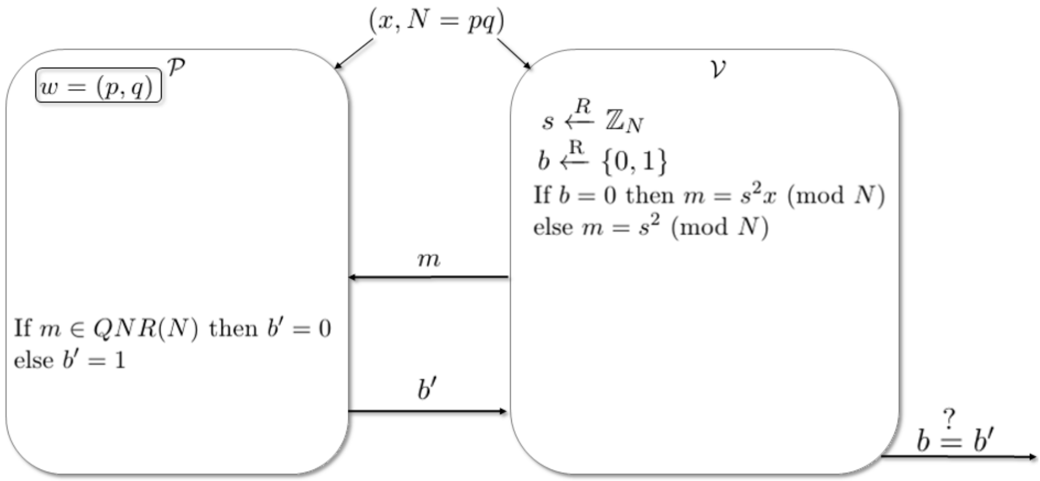
- Completeness: $\forall x \in L$
$$\Pr\left[Output_{\mathcal{V}}(\mathcal{P}(x) \leftrightarrow \mathcal{V}(x)) = 1\right] = 1$$
- Soundness: $\forall x \notin L$, $\forall \mathcal{P}^*$
$$\Pr\left[Output_{\mathcal{V}}(\mathcal{P}^*(x) \leftrightarrow \mathcal{V}(x)) = 1\right] \leq 1/2$$

a) Let IP$'$ be the class of languages where we allow the prover to be probabilistic i.e. the prover can use randomness. Show that IP$'$ = IP.

b) Let IP$'$ be the class of languages where we replace the 1/2 in the definition above by 0 i.e. the verifier must surely reject in case $x \notin L$. Show that IP$'$ = NP.

Problem 3 (34/100)

Consider the following protocol for showing that $x \in \mathbb{Z}_N$, for $N = pq$, is a quadratic nonresidue i.e. $\nexists y$ such that $x = y^2 \pmod N$.



That is,

Verifier: pick random $s \in \mathbb{Z}_N$, then with prob 1/2 send s^2 and with prob 1/2 send $s^2 x$.

Prover: tell whether received number is quadratic residue or not. Note that $QNR(N)$ is the set of quadratic nonresidues mod N.

Verifier: accept if sent s^2 and prover says residue or sent $s^2 x$ and prover says non-residue.

Note: for a prover with the factorization of N as its witness, $w = (p, q)$, it is easy for them to determine if $x \in \mathbb{Z}_N$ is a quadratic residue or not.

Show that the scheme is complete, sound, and honest verifier perfect zero-knowledge, but, unless the quadratic residuosity problem is in polynomial time, the scheme is not perfect zero knowledge.