24. Recall our definition of the class $IP_{\alpha,\beta}$: We say that a language $L \subseteq \{0,1\}^*$ is in this class if there is a polynomial-time verifier $V$ that uses a random string $r$ and has the following properties, where $P$ is an arbitrarily powerful prover that interacts with $V$:

$$
\begin{align*}
    x \notin L & \implies \forall P : \Pr_r[V \ast P(x, r) = 1] \leq \alpha, \\
    x \in L & \implies \exists P : \Pr_r[V \ast P(x, r) = 1] \geq \beta.
\end{align*}
$$

We defined $IP = IP_{\frac{3}{2}, 2}$ and remarked that the choice of the constants isn’t terribly important, as can be proven by suitable repetition and Chernoff bound analysis. We also remarked that $\beta$ can be made equal to 1 (perfect completeness), though not by simple repetition. Finally, we remarked that $\alpha$ cannot be made zero (perfect soundness), because that would boil the underlying class to plain old $NP$.

Justify this last remark. Specifically, prove that $IP_{0, \frac{3}{2}} = NP$. [2 points]

25. Let $p$ be a prime. This problem involves the group $\mathbb{Z}_p$, consisting of integers $\{1,2,\ldots,p-1\}$ with multiplication performed mod $p$. At some point you will need to use the fact that every element of $\mathbb{Z}_p$ has a multiplicative inverse mod $p$ (that’s what makes it a group).

The quadratic residuosity problem asks whether a given integer is a square mod $p$. The brute force solution is to try out all elements of $\mathbb{Z}_p$ and compute the square of each, but it takes time proportional to $p$, which is exponential in the input length. But one can give interesting interactive proofs for this problem. To be precise, define the languages

$$
\begin{align*}
    QR &= \{ \langle p,x \rangle : p \text{ is prime, } x \in \mathbb{Z}_p, \text{ and } \exists y \in \mathbb{Z}_p \ (y^2 \equiv x \ (mod \ p)) \}, \\
    QNR &= \{ \langle p,x \rangle : p \text{ is prime, } x \in \mathbb{Z}_p, \text{ and } \forall y \in \mathbb{Z}_p \ (y^2 \not\equiv x \ (mod \ p)) \}.
\end{align*}
$$

The acronyms denote “quadratic residue” and “quadratic non-residue,” respectively.

Prove that both these languages are in $IP$ and that one of these is in fact in $NP$. [2 points]

Hint: Your protocol for one of the languages should mimic the one we gave in class for $GNI$ (graph non-isomorphism). Suppose $\langle p,x \rangle \in QNR$ and $z \in \mathbb{Z}_p$. What can you say about $xz^2 \mod p$?