Problem 1:
Show that the size of the multiplicative group of $N = pq$ is $(p-1)(q-1)$.

Problem 2:
Show that if $p-1$ or $q-1$ was divisible by 3 then $k$ such that $3k \equiv 1 \mod (p-1)(q-1)$ would not exist.

Problem 3:
Given our knowledge of $p$ and $q$ how can we efficiently compute a cubed-root modulo $N$?

Problem 4:
In class we saw a zero knowledge proof for Graph Non-isomorphism. Give a Zero Knowledge proof for Graph Isomorphism.