**CSE 40622 Cryptography**
**Writing Assignment 05 (Lecture 09-10)**

Name: Walker Bagley (wbagley)

1. (20 pts, Page 4) In $\mathbb{Z}_p^*$ with an odd prime $p$, prove that a QR has exactly two square roots. That is, for any $x \in \mathbb{Z}_p^*$ that is a QR, there exists exactly two distinct $y$'s such that $y^2 = x$.

   - First show that a QR has at least two square roots, and then show that a QR has at most two square roots.
   - Hint: recall that $\mathbb{Z}_p^*$ has exactly $\frac{p-1}{2}$ QRs.

   **Answer:**

   *Proof.* Let $x$ be a QR in $\mathbb{Z}_p^*$, then there exists some $y \in \mathbb{Z}_p^*$ such that $y^2 = x$. Then we also know that $(-y)^2 = x$, so $x$ has at least two square roots. Consider two QRs $x_1, x_2$ that share a square root $y$. Then $y^2 = x_1 = x_2$, so $x_1 = x_2$. Thus, each QR has distinct square roots. Since we know that there are exactly $\frac{p-1}{2}$ QRs and $p-1$ elements in $\mathbb{Z}_p^*$ and each QR has at least 2 distinct roots that are not shared by any other QR, then each QR must have exactly 2 square roots. □

2. (20 pts, Page 6) Prove that, given $\mathbb{Z}_p^*$ with $p = 2q + 1$ where $p, q$ are both odd prime numbers, if a random number $g \in \mathbb{Z}_p^*$ satisfies $g \neq 1$ and $g^2 \mod p \neq 1$, $\langle g \rangle$ must be a subgroup of $\mathbb{Z}_p^*$ which contains ALL of QRs in $\mathbb{Z}_p^*$.

   - You need to prove all QRs of $\mathbb{Z}_p^*$ belong to $\langle g \rangle$. You do NOT need to prove $\langle g \rangle$ contains QRs only.

   **Answer:**

   *Proof.* Since the order of any subgroup must divide the order of the group, we know that $\mathsf{ord}(g)|\mathsf{ord}(\mathbb{Z}_p^*)$. Since it is given that the order of $g$ is neither 1 nor 2 and $|\mathbb{Z}_p^*| = 2q$ where $q$ is an odd prime, then $|\langle g \rangle|$ must be equal to either $q$ or $2q$. First, if $|\langle g \rangle| = 2q$, then $\langle g \rangle$ contains all elements of $\mathbb{Z}_p^*$ and thus all QRs. Second, if $|\langle g \rangle| = q$, then we know $g^q = 1$. Since 1 is a QR, we know that $g^q = y^2$ for some $y \in \mathbb{Z}_p^*$. Then $g^{\frac{q}{2}} = y$ but since $q$ is odd, $\frac{q}{2}$ is not an integer. So for this to hold, $g$ must be a QR, meaning $g = z^2$ for some $z \in \mathbb{Z}_p^*$. So, $g^q = (z^2)^q = 1$. Then since the subgroup generated by $g$ must contain elements expressed in powers of $g = z^2$, all elements of $\langle g \rangle$ are QRs. □

3. (10 pts, Coming from nowhere) Prove that any generator $g$ of $\mathbb{Z}_p^*$ is a QNR if $p$ is an odd prime number, WITHOUT using Corollary 1 in the note of Lecture 09-10.

   **Answer:**

   *Proof.* If $g$ generates $\mathbb{Z}_p^*$, then $|\langle g \rangle| = p - 1$. Suppose, towards a contradiction, that $g$ is a QR so there exists some $z$ where $z^2 = g$. Then $g^{p-1} = (z^2)^{p-1} = 1$ and every element generated by $g$ is of the form $z^{2k} = (z^k)^2$ meaning it is a QR. But we know that $g$ generates all of $\mathbb{Z}_p^*$, so it cannot generate only QRs. Here lies our contradiction, so $g$ must be a QNR. □

4. (10 pts, Page 6) What is the consequence if we have $p = kq + 1$ with a large positive even number $k$ instead of 2? In other words, what do you need to do **additionally** in order to find a generator of $\mathbb{Z}_p^*$?

   **Answer:**

   If $k$ is some large positive even number instead of just 2, we have more to check when looking for a generator. Instead of just checking whether $g^{\frac{p-1}{2}} \neq 1$ and $g^{\frac{p-1}{q}} \neq 1$, we must also check this for all other prime factors of $kq$. That is, for every prime factor $m$ of $kq$, we must ensure that $g^{\frac{p-1}{m}} \neq 1$ before we can say that $g$ is a generator.

5. (15 pts, Coming from nowhere) In class, I said one of the countermeasures to QR/QNR attacks is to use the subset of $\mathbb{Z}_p^*$ which contains all of its QRs and use it as $\mathbb{G}$ in ElGamal encryption. Then, Legendre symbols do not give much information to ciphertexts and public keys since all parameters will be QRs. Why is it not possible to use a subset of $\mathbb{Z}_p^*$ which contains all of its QNRs and use it as $\mathbb{G}$?

   **Answer:**

   The subset of $\mathbb{Z}_p^*$ containing only QNRs is not a subgroup as it is not closed under the group operator. Consider some $y$ QNR so that $y$ belongs to this subset. If the QNRs formed a subgroup, then $y^2$ would also be in this subset, but it is obvious that $y^2$ is a QR and thus is not contained in the QNR subset. Since the QNR subset does not form a group, it is impossible to use it as a group in ElGamal encryption.