Solution to **Exercise 15** of Homework 5

p prime, g a primitive element (PE) modulo p, $a, b \in \mathbb{Z}_p^*$

(a) a QR $\mod p \Leftrightarrow \exists i \in \mathbb{N}_0$ with $a \equiv g^{2i} \pmod p$

"$\Rightarrow$":

$$\begin{aligned} &a \text{ QR} \mod p \Rightarrow \exists k \in \mathbb{Z}_p^* : k^2 \equiv a \pmod p \\ &g \text{ PE} \Rightarrow \exists l \in \mathbb{N}_0 : k = g^l \Rightarrow k^2 \equiv g^{2l} \equiv a \pmod p \end{aligned}$$

"$\Leftarrow$":

$$\begin{aligned} \exists i \in \mathbb{N}_0 \text{ with } a \equiv g^{2i} \pmod p &\Rightarrow a \equiv (g^i)^2 \pmod p \\ &\Rightarrow a \text{ is QR} \mod p \end{aligned}$$

(b) If p is odd, then exactly one half of elements $x \in \mathbb{Z}_p^*$ are QRs $\mod p$.

- p even: $|\mathbb{Z}_2^*| = 1$
- p odd: $|\mathbb{Z}_p^*| = p - 1$ is even

$$\begin{aligned} &\mathbb{Z}_p^* =< g >= \{g^0, g^1, g^2, \ldots, g^{p-2}\} \\ &A = \{g^0, g^2, g^4, \ldots, g^{p-3}\} \Rightarrow |A| = \frac{p-1}{2} \end{aligned}$$

- $x \in A \Rightarrow \exists i \in \mathbb{N}_0$ with $x \equiv g^{2i} \pmod p \overset{(a)}{\Rightarrow} x$ QR $\mod p$
- $x \in \mathbb{Z}_p^* \setminus A$: Assumption x is QR $\mod p$

$$\begin{aligned} &\overset{(a)}{\Rightarrow} \exists i \in \mathbb{N}_0 \text{ with } x \equiv g^{2i} \pmod p \\ &\Rightarrow x \in A \Rightarrow \text{Contradiction (Note: } 2i \mod (p-1) \text{ is even)} \end{aligned}$$

(c) ab QR $\mod p \Leftrightarrow a, b$ QR $\mod p$ or a, b NQR $\mod p$

"$\Rightarrow$": $a \equiv g^k, b \equiv g^l \pmod p$

$$\begin{aligned} ab \text{ QR} \mod p &\Rightarrow \exists i \in \mathbb{N}_0 \text{ with } ab \equiv g^{2i} \pmod p \\ &\Leftrightarrow ab \equiv g^{k+l} \equiv g^{2i} \pmod p \\ &\Rightarrow k + l \equiv 2i \pmod{p-1} \\ &\Rightarrow \begin{cases} k, l \text{ even} \\ \vee\, k, l \text{ odd} \end{cases} \overset{(a)}{\Rightarrow} \begin{cases} a, b \text{ QR} \mod p \\ \vee\, a, b \text{ NQR} \mod p \end{cases} \end{aligned}$$

"$\Leftarrow$":

$$\begin{aligned} a, b \text{ QR} \mod p &\Rightarrow a \cdot b \equiv g^{2k} \cdot g^{2l} \equiv g^{2(k+l)} \pmod p \\ &\overset{(a)}{\Rightarrow} ab \text{ QR} \mod p \end{aligned}$$

$$\begin{aligned} a, b \text{ NQR} \mod p &\Rightarrow a \cdot b \equiv g^{2k+1} \cdot g^{2l+1} \equiv g^{2(k+l+1)} \pmod p \\ &\overset{(a)}{\Rightarrow} ab \text{ QR} \mod p \end{aligned}$$