1. (a) To show $QR \leq \mathbb{Z}_p^*$ it is enough to show (i) $1 \in QR$, (ii) closure under multiplication, and (iii) closure under inversion.

   i. Indeed $1 \in QR$, because $1 \equiv 1^2 \pmod{p}$

   ii. Let $s_1, s_2 \in QR$. Then are $r_1, r_2 \in \mathbb{Z}_p^*$ s.t. $s_1 \equiv r_1^2 \pmod{p}$, $s_2 \equiv r_2^2 \pmod{p}$. Then follows:

$$s_1 s_2 \equiv r_1^2 r_2^2 = (r_1 r_2)^2 \pmod{p}$$

   and $r_1 r_2 \in \mathbb{Z}_p^*$ because $\mathbb{Z}_p^*$ is a group. Therefore $s_1 s_2 \in QR$ by definition.

   iii. Let $s \in \mathbb{Z}_p^*$. Then there is $r \in \mathbb{Z}_p^*$ s.t. $s \equiv r^2 \pmod{p}$. Therefore:

$$s^{-1} \equiv \left(r^2\right)^{-1} = \left(r^{-1}\right)^2 \pmod{p}$$

   and $r^{-1} \in \mathbb{Z}_p^*$, therefore$s^{-1} \in QR$.

(b) Let $g \in \mathbb{Z}_p^*$, $\mathbb{Z}_p^* = \langle g \rangle$. Assume by contradiction that $g \in QR$. Then there is an $r \in \mathbb{Z}_p^*$ s.t. $g \equiv r^2 \pmod{p}$. Because $g$ generates $\mathbb{Z}_p^*$ there exists $i \in \mathbb{Z}$ s.t. $r \equiv g^i \pmod{p}$ . Therefore $g \equiv g^{2i} \pmod{p} \iff g^{2i-1} \equiv 1 \pmod{p}$. Therefore $2i - 1 | o(g) = \varphi(p) = p - 1$. Note that for prime $p > 2$ we know $p$ is odd, therefore $p - 1$ is even. On the other hand $2i - 1$ is odd, therefore we get a contradiction (that odd divides even), meaning $g \notin QR$. For the edge case where $p = 2$, $\mathbb{Z}_p^*$ is the trivial group (of 1 element), and in this case the claim is not true (because $\mathbb{Z}_p^* = QR = \langle 1 \rangle$). From now on we will assume $p > 2$.

(c) Let $g \in \mathbb{Z}_p^*$, $\mathbb{Z}_p^* = \langle g \rangle$.

   i. Let $a \in \mathbb{Z}_p^*$. Assume $a \in QR$. Then there exists $r \in \mathbb{Z}_p^*$ s.t. $a \equiv r^2 \pmod{p}$. Because $g$ generates $\mathbb{Z}_p^*$, there exists a $k \in \mathbb{Z}$ s.t. $r \equiv g^k \pmod{p}$. Therefore $a \equiv r^2 \equiv \left(g^k\right)^2 = g^{2k} \pmod{p}$.

   ii. Let $a \in \mathbb{Z}_p^*$. Assume that $a \equiv g^{2k} \pmod{p}$ for some k. Then $a \equiv \left(g^k\right)^2 \pmod{p}$, $g^k \in \mathbb{Z}_p^*$, therefore by definition $a \in QR$.

(d) Let $a \in \mathbb{Z}_p^*$, $\mathbb{Z}_p^* = \langle g \rangle$.

   i. Assume $a \in QR$. Then by (c) there is a $k \in \mathbb{Z}$ s.t. $a \equiv g^{2k} \pmod{p}$. Therefore

$$a^{\frac{p-1}{2}} \equiv \left(g^{2k}\right)^{\frac{p-1}{2}} = \left(g^{p-1}\right)^k \equiv 1^k = 1 \pmod{p}$$

   (Note that $g^{p-1} \equiv 1$ because $o(g) = p - 1$)

   ii. Assume $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$. There is an $i \in \mathbb{Z}$ s.t. $a \equiv g^i \pmod{p}$. Therefore

$$1 \equiv \left(g^i\right)^{\frac{p-1}{2}} = \left(g^{\frac{p-1}{2}}\right)^i \stackrel{*}{=} (-1)^i \pmod{p}$$

   Thus $i$ is even (again assuming $p > 2$). Denote $i = 2k$, and now by (c) we get that $a \in QR$.

   * - This can be explained as follows: $g^{\frac{p-1}{2}} \not\equiv 1$ because $o(g) = p - 1 > \frac{p-1}{2}$, and $\left(g^{\frac{p-1}{2}}\right)^2 = g^{p-1} \equiv 1$. Therefore necessarily $g^{\frac{p-1}{2}} \equiv -1$, because $\pm 1$ are the only square roots of $1 \pmod{p}$ . (There are no other roots because $x^2 - 1$ as at most 2 roots)

(e) Denote $a = g^x \mod p$. Then x is even $\iff$ there is a $k \in \mathbb{Z}$ s.t. $x = 2k \iff a \in QR$ (by c) $\iff a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$ (by d).

   Therefore given $f(x) = g^x \mod p$ we can compute $b := (f(x))^{\frac{p-1}{2}} \mod p$. If $b = 1$ then necessarily x is even, i.e. $parity(x) = 0$. Otherwise (if $b = 0$) x is odd, i.e. $parity(x) = 1$.

   $a^n \mod p$ can be computed efficiently as follows: compute values $a^{2^k}$ iteratively by squaring (mod p), until $2^k \geq n$ (note that we don't have to store $a^{2^k}$ in memory, as we compute (mod p)). Then according to the binary representation of $n$, multiply these values for which the k'th bit of $n$ is 1. The whole process involves $O(\log_2(n))$ multiplications mod p, which is linear in the number of bits of $n$.