8.1.2(b) If a has order $2k$ modulo the odd prime p, then $a^k \equiv -1 \pmod{p}$.

Suppose that a has order $2k$ modulo the odd prime p. Then $a^{2k} \equiv 1 \pmod{p}$. Then $a^{2k} - 1 \equiv 0 \pmod{p}$. So $(a^k - 1)(a^k + 1) \equiv 0 \pmod{p}$, i.e. $p \mid (a^k - 1)(a^k + 1)$. Since p is prime, p must divide one of $a^k - 1$ and $a^k + 1$. If $p \mid (a^k - 1)$, then $a^k \equiv 1 \pmod{p}$, contradicting our assumption. Thus $p \mid (a^k + 1)$, i.e. $a^k \equiv -1 \pmod{p}$.

8.1.8(a) Prove that if p and q are odd primes and $q \mid a^p - 1$, then either $q \mid a - 1$ or else $q = 2kp + 1$ for some integer k. [Hint: Because $a^p \equiv 1 \pmod{q}$, the order of a modulo q is either 1 or p; in the latter case, $p \mid \phi(q)$.]

Notice that $\gcd(a, q) = 1$. To show this, assume for the sake of contradiction that $\gcd(a, q) = d$ with $d > 1$. Then $d \mid q$ and $q \mid a^p - 1$ give that $d \mid a^p - 1$. Since $d \mid a$, we have $d \mid 1$, a contradiction. Hence $\gcd(a, q) = 1$. Since $q \mid a^p - 1$, we know $a^p \equiv 1 \pmod{q}$. Pick t to be the order of a modulo q. Then $t \mid p$. Since p is prime, we know that $t = 1$ or $t = p$. Suppose that $t = 1$. Then $a \equiv 1 \pmod{q}$ or $q \mid (a - 1)$. Now suppose that $t = p$. With $a^{\phi(q)} \equiv 1 \pmod{q}$ since $\gcd(a, q) = 1$, we know $p \mid \phi(q)$. Notice that $\phi(q) = q - 1$ which implies that $p \mid q - 1$. So there exists a $r \in \mathbb{Z}$ such that $pr = q - 1$. Since q is odd, $q - 1$ is even. Since p is odd, r must be even. So $r = 2k$ for some $k \in \mathbb{Z}$. Then

$$pr = p(2k) = q - 1$$

gives

$$q = 2kp + 1,$$

as desired.

8.1.10 Let r be a primitive root of the integer n. Prove that r^k is a primitive root of n if and only if $\gcd(k, \phi(n)) = 1$.

Let r be a primitive root of the integer n. Then r has order $\phi(n)$ modulo n. Theorem 8.3 gives that r^k has order $\phi(n)/\gcd(k, \phi(n))$. Suppose that r^k is a primitive root of n. Then r^k has order $\phi(n)$. Theorem 8.3 gives that

$$\phi(n) = \phi(n)/\gcd(k, \phi(n))$$

which implies that $\gcd(k, \phi(n)) = 1$.

Suppose that $\gcd(k, \phi(n)) = 1$. Then r^k has order $\phi(n)$ by theorem 8.3. So r^k is a primitive root of n.