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

Proof. Let p be an odd prime and $a^{2k} \equiv 1$ (mod p). Notice,

$$(a^k)^2 - 1 \equiv 0 \pmod{p} \Rightarrow (a^k - 1)(a^k + 1) \equiv 0 \text{ (mod p)}$$

Then, $p|(a^k - 1)(a^k + 1) \Rightarrow p|(a^k + 1)$. So, $a^k \equiv -1 \pmod{p}$
Therefore, If a has order $2k$ modulo the odd prime p, then $a^k \equiv -1 \pmod{p}$ □

8.1.8a Prove that if p and q are odd primes and $q|a^p - 1$, then either $q|a - 1$ or else $q = 2kp + 1$ for some integer k.

Proof. Let p and q be odd primes and $q|a^p - 1$ Note, $\gcd(a, q) = 1$ and $a^p \equiv 1 \pmod{q}$. Let r be the order of a modulo q. Then, $r|p$. As p is prime, we have $r = 1$ or $r = p$. If $r = 1$, we have $a \equiv 1 \pmod{q} \Rightarrow q|(a - 1)$
If $r = p$, we have $a^{\phi(q)} \equiv 1 \pmod{q}$. Then, $p|\phi(q) \Rightarrow p|q - 1$. There must be some m such that $pm = q - 1$. As q is odd, $q - 1$ must be even, and as p is odd, m must be even, so $m = 2k$ for some $k \in \mathbb{Z}$.
Thus, $p(2k) = q - 1 \Rightarrow q = 2pk + 1$.
Therefore, if p and q are odd primes and $q|a^p - 1$, then either $q|a - 1$ or else $q = 2kp + 1$ for some integer k □

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

Proof. As r has order $\phi(n) \pmod{n}$, we then have r^k has order $\phi(n)/\gcd(k, \phi(n))$.

Assume $\gcd(k, \phi(n)) = 1$ then r^k has order $\phi(n)$.
Thus, r^k is a primitive root of n

Suppose r^k is a primitive root of n. Then r^k has order $\phi(n)$.As $\phi(n)$ is $\phi(n)/\gcd(k, \phi(n))$.
Thus, $\gcd(k, \phi(n)) = 1$.

Therefore, r^k is a primitive root of n if and only if $\gcd(k, \phi(n)) = 1$. □