Page 107 Problem 3: Let a, b, c be integers. Let $a^b \equiv a^c \pmod{n}$ with $(a, n) = 1$. Assume that b and c are least residues mod n. If $b = c$, then certainly $b \equiv c \bmod \pmod{ord_n(a)}$ and we are done. Assume that $b \neq c$ and without loss of generality, let $c < b$. Then

$$(a^b)a^{-c} \equiv (a^c)a^{-c} \pmod{n}$$
$$a^{b-c} \equiv 1 \pmod{n}$$

Since b and c are least residues, $b - c$ is a least residue mod n and hence by definition, $ord_n(a) = b - c$. Then

$$b - c = ord_n(a)(1)$$
$$ord_n(a)|b - c$$
$$b \equiv c \pmod{ord_n(a)}$$

Thus the theorem is satisfied. Suppose instead that $b \equiv c \pmod{ord_n(a)}$. Then by definition, $ord_n(a)|b - c$ which implies $b - c = ord_n(a)k$ for some least reside $k \in \mathbb{Z}$. Since all terms are least residues, we have

$$a^{b-c} \equiv a^{ord_n(a)\cdot k} \pmod{n}$$
$$a^b a^{-c} \equiv 1^k \pmod{n}$$
$$a^b a^{-c} a^c \equiv a^c(1) \pmod{n}$$
$$a^b \equiv a^c \pmod{n}$$

Therefore, the theorem has been proven.

Page 107 Problem 7: Let g be a primitive root of n and let $G = \{g, g^2, g^3, ...g^{\phi(n)}\}$. Since $(g, n) = 1$, it would follow that each element of G is also relatively prime to n, simply because if g and n share no common divisors, then certainly the product of multiple g's and n still share no common divisors. Then by definition, G is a reduced residue system (RRS) of n if and only if each of the $n-1$ elements of G are distinct from one another (definition on page 58). To prove this, we will use proof by contradiction. Suppose that two elements of G are equal to one another, that is $g^j \equiv q^k \pmod{n}$ for some $0 < k < j \leq \phi(n)$. Then

$$(g^k)g^{-j} \equiv (g^j)g^{-j} \pmod{n}$$
$$g^{k-j} \equiv 1 \pmod{n}$$

But, this equivalence is impossible since the order of g is $\phi(n)$ (as specified by the fact that g is a primitive root) and $k-j < \phi(n)$. Thus it is impossible for g to be a primitive root and hence G is not a RRS since two elements are equal to one another mod n. By contradiction we have shown that G is a RRS if and only if each element of G is distinct mod n. Therefore we have proven the theorem.

Page 107 Problem 11: Let n be a positive integer with the primitive root a. If there is another primitive root of n, then it must be in the set $A = \{a, a^2, a^3, ..., a^{\phi(n)}\}$ since A is a complete residue set of n by problem 7 above. To show that a number a^k is a primitive root for $1 \leq k \leq \phi(n)$, we need to show that a^k is a primitive root if and only if $(k, \phi(n)) = 1$. Suppose that k is relatively prime to $\phi(n)$. Then by Bezout's Theorem there exist integers s, t such that $ks = t\phi(n) + 1$. It follows that

$$\begin{gathered} g^{ks} = (g^{t\phi(n)} + 1) \equiv g \pmod{n} \\ g^{ks} \equiv (g^{t\phi(n)})g \pmod{n} \\ g^{ks} \equiv g(1^t) \equiv g \pmod{n} \end{gathered}$$

Since $g^{ks} \equiv g \pmod{n}$, for any integer r we have $g^r \equiv (g^{ks})^r \equiv (g^k)^{sr} \pmod{n}$. Therefore any power of g is congruent to some power of g^k which thus implies that g^k is a primitive root of n.

Alternatively, suppose that k and $\phi(n)$ are not relatively prime. Let $d > 1$ be a common divisor. Then $g^{k\phi(n)/d} \equiv 1^{k/d} \equiv 1 \pmod{n}$ since $k\phi(n)/d$ is a multiple of $\phi(n)$. Then by definition this implies that g^k has order less than $\phi(n)/d$ so g^k cannot be a primitive root.

Thus, we have shown that g^k is a primitive root if and only if $(g^k, \phi(n)) = 1$. The number of elements less than $\phi(n)$ that are relatively prime to $\phi(n)$ is given by: $\phi(\phi(n))$. Thus we have proven the theorem.

Page 108 Problem 2: Let n be an integer greater than 2 and let $n = p_1^{a_1} p_2^{a_2} ... p_k^{a_k}$ be the prime factorization of n. Suppose that n has as least one odd prime factor, $p_i^{a_i}$ for $1 \leq i \leq k$. By the lemma below, both $p_i^{a_i}$ and $p_i^{a_i - 1}$ are odd numbers. So $\phi(p_i^{a_i}) = (p^{a_i} - p_i^{a_i - 1})$ is an even number since an odd number minus an odd number is always even. Therefore $\phi(p_i^{a_i})$ is even and has a factor of 2, thus, $\phi(n)$ has at least one even factor and is divisible by

2.

Suppose that n has no odd prime factors. Then its only prime factor must be 2. Let $n = 2^c$ for some $c \in \mathbb{Z}_+$. Then $\phi(n) = \phi(2^c) = (2^c - 2^{c-1})$. Since 2 to any positive integer power is always even (by the lemma below), $2^c - 2^{c-1}$ is even. Then $\phi(n)$ is even and is divisible by 2 and the theorem has been proven in all possible cases.

Lemma: If a is an odd integer, then a^n is always odd for $n \in \mathbb{Z}_+$
Let a be an odd integer. In the case that $a = 5$, it is certainly true that $5^1 = 5$, $5^2 = 25$, $5^3 = 125$... are all odd numbers. Now, suppose that a^k is odd for some a and for some $k > 1$. To prove this lemma, it suffices to prove that $a^{k+1} \equiv 1 \pmod 2$. From our base case, we have $a^1 \equiv 1 \pmod 2$, and from the inductive step, we have $a^k \equiv 1 \pmod 2$. From theorem 3.2, if $a \equiv b \pmod n$ and $c \equiv d \pmod n$, then $ac \equiv bd \pmod n$. Thus, we have $a \cdot a^k \equiv 1 \cdot 1 \pmod 2$ which is equivalent to $a^{k+1} \equiv 1 \pmod 2$. Therefore, we have proven the theorem by induction and a^n is odd.

Lemma: Any positive integer power of 2 is even.
First, observe that $2^1 = 2$ is even, so $2^1 \equiv 0 \pmod 2$. Next, suppose that 2^n is even for some $n \in \mathbb{Z}_+$, $n > 1$. Then $2^n \equiv 0 \pmod 2$. Notice that $2^{n+1} = 2^n \cdot 2^1 \equiv 0 \cdot 0 \pmod 2$ by theorem 3.2. Therefore $2^{n+1} \equiv 0 \pmod 2$ is even and thus the theorem is proven.

Page 108 Problem 5: Suppose that p is an odd prime and that g is a primitive root of p^k for some positive integer k. That is, g satisfies $(g, p^k) = 1$ and $ord_{p^k}(g) = \phi(p^k)$. Using the result from problem 4, we have

$$\begin{aligned}
(g+p)^{\phi(p^k)} &\equiv g^{\phi(p^k)} - p^k g^{\phi(p^k)-1} \pmod{p^{k+1}} \\
p(g+p)^{\phi(p^k)} &\equiv pg^{\phi(p^k)} - p^{k+1} g^{\phi(p^k)-1} \pmod{p^{k+1}} \\
p(g+p)^{\phi(p^k)} &\equiv pg^{\phi(p^k)} \pmod{p^{k+1}} \\
p^{-1}p(g+p)^{\phi(p^k)} &\equiv p^{-1}pg^{\phi(p^k)} \pmod{p^{k+1}} \\
(g+p)^{\phi(p^k)} &\equiv g^{\phi(p^k)} \pmod{p^{k+1}} \\
((g+p)^{\phi(p^k)})^p &\equiv (g^{\phi(p^k)})^p \pmod{p^{k+1}} \\
(g+p)^{p(p^k - p^{k-1})} &\equiv g^{p(p^k - p^{k-1})} \pmod{p^{k+1}} \\
(g+p)^{p^{k+1} - p^k} &\equiv g^{p^{k+1} - p^k} \pmod{p^{k+1}} \\
(g+p)^{\phi(p^{k+1})} &\equiv g^{\phi(p^{k+1})} \pmod{p^{k+1}}
\end{aligned}$$

Since $(g, p^k) = 1$, it follows that $(g, p^{k+1}) = 1$. Therefore, we can use Euler's Theorem:

$$(g+p)^{\phi(p^{k+1})} \equiv g^{\phi(p^{k+1})} \equiv 1 \pmod{p^{k+1}}$$

Thus we have shown that both g and $g+p$ are primitives root of p^{k+1} since $ord_{p^{k+1}}(g) = \phi(p^{k+1})$ and $ord_{p^{k+1}}(g+p) = \phi(p^{k+1})$. We have iteratively shown that primitive roots are the same for different powers of the same odd prime and have thus proven the theorem.

Page 108 Problem 6: Let p be an odd prime. By the previous problem, p^n has a primitive root, call it g, such that $g^{\phi(p^n)} \equiv 1 \pmod{p^n}$. We will prove that g is also a primitive root of $2p^n$.

Suppose that g is a primitive root of $2p^n$. Then by definition, g must satisfy $(g, 2p^n) = 1$. If g is relatively prime to $2p^n$, then g must be odd, otherwise, they would share a common factor of 2. Let $m = ord_{2p^n}(g)$. Then g must also satisfy $g^m \equiv 1 \pmod{2p^n}$. Observe that $\phi(2p^n) = \phi(2)\phi(p^n) = \phi(p^n)$, so it follows from exercise 5 that $g^m \equiv 1 \pmod{p^n}$. By definition, this means that $p^n | g^m - 1$. Since we found g to be odd, $g^m - 1$ is even as a consequence of the lemma proven above, and $2|g^m - 1$. If $2|g^m - 1$ and $p^n|g^m - 1$, then it is true that $2p^n|g^m - 1$, which gives $g^m \equiv 1 \pmod{2p^n}$. Therefore, g is a primitive root of $2p^n$ since $(g, 2p^n) = 1$ and the order of g is $m = \phi(2p^n)$.

What if g is not odd? If g is not odd, let $G = g + p^n$ and let $\phi(p^n) = \phi(2p^n) = m$. By theorem 2.4, $(G, p^n) = 1$ and by Euler's Theorem,

$$G^{\phi(p^n)} \equiv 1 \pmod{p^n}$$
$$p^n | G^m - 1$$

Again, since p^n is odd by the lemma and g is even by proposition, G is odd. Therefore, G^m is odd and $G^m - 1$ is even, so $2|G^m - 1$. If $p^n|G^m - 1$ and $2|G^m - 1$ then $2p^n|G^m - 1$. It follows that $G^{\phi(2p^n)} \equiv 1 \pmod{2p^2}$. Therefore all conditions of a primitive root have been met and the theorem has been proven.