8.2.1 (b) If p is an odd prime, prove that the congruence $x^{p-2} + \cdots + x^2 + x + 1 \equiv 0 \pmod{p}$ has exactly $p-2$ incongruent solutions, and they are the integers $2, 3, \ldots, p-1$.

Observe that $x^{p-1} - 1 \equiv 0 \pmod{p}$ has exactly $p-1$ solutions, namely $1, 2, \ldots, p-1$. Notice $x^{p-1} - 1 = (x-1)(x^{p-2} + \cdots + x + 1)$. Since $x - 1 \equiv 0 \pmod{p}$ has exactly one solution $x \equiv 1 \pmod{p}$, we know that $x^{p-2} + \cdots + x + 1 \equiv 0 \pmod{p}$ must have exactly $(p-1) - 1 = p-2$ solutions. Since $x \not\equiv 1 \pmod{p}$ for $x = 2, 3, \ldots, p-1$ and $x^{p-1} - 1 \equiv 0 \pmod{p}$ for $x = 2, 3, \ldots, p-1$, we have that $x^{p-2} + \cdots + x^2 + x + 1 \equiv 0 \pmod{p}$ for $x = 2, 3, \ldots, p-1$, as desired.

8.2.2 (b) Verify $x^2 \equiv -1 \pmod{65}$ has four incongruent solutions.

Note that $65 = 5 \cdot 13$ and $x^2 \equiv -1 \pmod{65}$ is the same as $x^2 + 1 \equiv 0 \pmod{65}$. Since 5 and 13 are both primes, we can rewrite these as $x^2 - 4 \equiv 0 \pmod{5}$ and $x^2 - 25 \equiv 0 \pmod{13}$. Then we want to know when $5 \mid (x-2)(x+2)$ and $13 \mid (x-5)(x+5)$. So, $x \equiv 2 \pmod{5}$ or $x \equiv 3 \pmod{5}$. Also, $x \equiv 5 \pmod{13}$ or $x \equiv 8 \pmod{13}$. By the Chinese Remainder Theorem, the solutions must be $x_1 \equiv 8 \pmod{65}$, $x_2 \equiv 18 \pmod{65}$, $x_3 \equiv 47 \pmod{65}$, and $x_4 \equiv 57 \pmod{65}$.

8.2.3 (b) Determine all the primitive roots of the prime $p = 19$, expressing each as a power of some one of the roots.

We want to know the values of a that satisfy $a^{\phi(19)} = a^{18} \equiv 1 \pmod{19}$ with $\phi(19)$ being the least such power that this equation holds. Note that 2 is a primitive root as $2^{18} \equiv 1 \pmod{19}$ has that 18 is the smallest such power satisfying this congruence. Then we know that the other primitive roots of 19 are congruent to 2^h when $\gcd(h, 18) = 1$ by theorem 8.3. So, $\gcd(h, 18) = 1$ when $h = 1, 5, 7, 11, 13, 17$. So, the remaining primitive roots are 2^5, 2^7, 2^{11}, 2^{13}, and 2^{17}. So, all of the primitive roots of 19 are 2, $13 \equiv 2^5 \pmod{19}$, $14 \equiv 2^7 \pmod{19}$, $15 \equiv 2^{11} \pmod{19}$, $3 \equiv 2^{13} \pmod{19}$, and $10 \equiv 2^{17} \pmod{19}$. Note: there are exactly $\phi(\phi(19)) = \phi(18) = \phi(3^2) \cdot \phi(2) = 6$ primitive roots.

8.2.6 (a) Assuming that r is a primitive root of the odd prime p, establish the congruence $r^{(p-1)/2} \equiv -1 \pmod{p}$ holds.

Suppose that r is a primitive root of the odd prime p. Then $r^{\phi(p)} = r^{p-1} \equiv 1 \pmod{p}$. Since p is odd, we know that $(p-1)/2$ is an integer. So $r^{p-1} - 1 \equiv 0 \pmod{p}$ implies that $(r^{(p-1)/2} - 1)(r^{(p-1)/2} + 1) \equiv 0 \pmod{p}$. If $r^{(p-1)/2} - 1 \equiv 0 \pmod{p}$, then r would not be a primitive root as $(p-1)/2 < p-1$ would contradict our assumption. So

$$r^{(p-1)/2} + 1 \equiv 0 \pmod{p}$$

which implies

$$r^{(p-1)/2} \equiv -1 \pmod{p}.$$