8.2.1b If p is an odd prime, then 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 $2, 3, \cdots, p-1$

Proof. Notice, as p is an odd prime and for $1 \leq x \leq p-1$, we have $\gcd(x,p) = 1$. Then by Fermat's Theorem we have $x^{p-1} \equiv 1 \pmod{p} \Rightarrow x^{p-1} - 1 \equiv 0 \pmod{p}$ has exactly $p-1$ solutions. Notice,

$$x^{p-1} = (x-1)(x^{p-2} + x^{p-3} + \cdots + x^2 + x + 1)$$

Then $x - 1 \equiv 0 \pmod{p}$ has exactly 1 solution. Also, we then have $x^{p-2} + \cdots + x + 1$ has exactly $(p-1) - 1 = p-2$ solutions. As $x \not\equiv 1 \pmod{p}$ for $2 \leq x \leq p-1$ and $x^{p-1} - 1 \equiv 0$ for $2 \leq x \leq p-1$. Then, $x^{p-2} + \cdots + x + 1 \equiv 0$
Therefore, 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 $2, 3, \cdots, p-1$ □

8.2.2b Verify the congruence $x^2 \equiv -1 \pmod{65}$ has four incongruent solutions; hence, Lagrange's theorem need not hold if the modulus is a composite number.
Note, $65 = 5 \cdot 13$. Then

$$\begin{aligned} x^2 &\equiv -1 \pmod{5} & x^2 &\equiv -1 \pmod{13} \\ x^2 &\equiv 4 \pmod{5} & x^2 &\equiv 12, x^2 \equiv 25 \pmod{13} \\ (x+2)(x-2) &\equiv 0 \pmod{5} & (x+5)(x-5) &\equiv 0 \pmod{13} \end{aligned}$$

Thus, $x \equiv 8, 18, 47, 57 \pmod{65}$

8.2.3b Determine the roots of the prime $p = 19$ expressing p as a power of some one of the roots.
Notice, $\phi(p-1) = \phi(18) = 6$. Then we have $x^{18} \equiv 1 \pmod{19}$. We then have $x = 2$ being a primitive root. Determining the rest we have 2^k where $k \in \mathbb{Z}$ and $\gcd(k, 18) = 1$. Thus, $k = 1, 5, 7, 11, 13, 17$
Therefore, the primitive roots are $2^1, 2^5, 2^7, 2^{11}, 2^{13}, 2^{17}$

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

Proof. Note, that by Fermat's Theorem we have $r^{p-1} \equiv 1 \pmod{p}$. Then,

$$p | r^{p-1} - 1 = (r^{(p-1)/2} - 1)(r^{(p-1)/2} + 1)$$

Notice, that $p \nmid r^{(p-1)/2} - 1$, as then $r^{(p-1)/2} \equiv 1 \pmod{p}$, which implies that r is not a primitive root.
Therefore, we must have $r^{(p-1)/2} \equiv -1 \pmod{p}$.

□