Problem 3): Since $\mathbb{Z}_{\mathfrak{p}}^{\star} \equiv \{a \in \{1, 2, \ldots, \mathfrak{p} - 1\} \,|\, \gcd(a, \mathfrak{p}) = 1\}$, for any $\mathfrak{p} \in \mathbb{Z}^{+}$, the set of possible elements for $\mathbb{Z}_{p^e}^{\star}$ is defined as

$$\mathbb{Z}_{p^e}^{\star} \subset \{1, 2, \ldots, p^e - 1\} \tag{3.1}$$

This implies the following relation between the cardinalities of these sets

$$|\mathbb{Z}_{p^e}^{\star}| < |\{1, 2, \ldots, p^e - 1\}|,$$

where $|\{1, 2, \ldots, p^e - 1\}|$ has the value $|\{1, 2, \ldots, p^e - 1\}| = (p^e - 1)$. It follows that the value of $|\mathbb{Z}_{p^e}^{\star}|$ can be obtained by determining the set of all values in $\{1, 2, \ldots, p^e - 1\}$ that do not satisfy the conition given in 3.1 and subtracting the cardinality of this set from $(p^e - 1)$. Since the common multiple is p, we will write this set in terms of be. Thus, the set of values in $\{1, 2, \ldots, p^e - 1\}$ that do not satisfy the condition in 3.1 may be defined as

$$\left\{p, 2p, 3p, \ldots, p\,p, 2p\,p, 3p\,p, \ldots, p^2\,p, \ldots, \left(p^{e-1} - 1\right)\ p\right\}$$

This definition arises becuase only multiples of p do not satistfy the condition in 3.1 and because $\left(p^{e-1} - 1\right)\ p = p^e - p$ is the largest element of $\{1, 2, \ldots, p^e - 1\}$ that does not satisfy the confition in 3.1. The cardinality of this set, $\left\{p, 2p, 3p, \ldots, p\,p, 2p\,p, 3p\,p, \ldots, p^2\,p, \ldots, \left(p^{e-1} - 1\right)\ p\right\}$ is clearly

$$|\left\{p, 2p, 3p, \ldots, p\,p, 2p\,p, 3p\,p, \ldots, p^2\,p, \ldots, \left(p^{e-1} - 1\right)\ p\right\}| = \left(p^{e-1} - 1\right)$$

Subtracting this value from $|\{1, 2, \ldots, p^e - 1\}| = (p^e - 1)$ finally yields

$$\phi(p^e) = (p^e - 1) - \left(p^{e-1} - 1\right) = p^e - 1 - p^{e-1} + 1 = p^e - p^{e-1} = p^{e-1}(p - 1)$$

as desired.

To show that

$$\phi\left(pq\right) = \phi\left(p\right)\ \phi\left(q\right)$$

holds for any relatively prime p and q, we apply a similarly strategy to the one used above. The number of possible elements of $\mathbb{Z}_{pq}^{\star}$ is $pq - 1$. As before, we must take into account that some possible elements of $\mathbb{Z}_{pq}^{\star}$ will not satisfy the definition in 3.1. If we subtract the number of these elements, then we will have $\phi\left(pq\right) = |\mathbb{Z}_{pq}^{\star}|$. Since there are $p - 1$ multiples of q that do not satisfy the condition in 3.1, we must subtract $p - 1$ from $pq - 1$. Similarly, since there are also $q - 1$ multiples of p that do not satisfy the same condition, we must also subtract $q - 1$ from $pq - 1$. Carrying out these subtractions gives

$$\begin{aligned}
\phi\left(pq\right) &= \left(pq - 1\right) - \left(p - 1\right) - \left(q - 1\right) \\
&= pq - 1 - p + 1 - q + 1 \\
&= pq - p - q + 1 \\
&= \left(p - 1\right)\left(q - 1\right) \\
&= \phi\left(p\right)\ \phi\left(q\right)
\end{aligned}$$

since $\phi\left(p\right)$ and $\phi\left(q\right)$ are defined as $\phi\left(p\right) = p - 1$ and $\phi\left(q\right) = q - 1$, respectively.

We will now use the previous result to show that, for an integer $N = \prod_i \left\{p_i^{e_i}\right\}$ and p_i distinct primes, we have

$$\phi\left(N\right) = \prod_i \left\{p_i^{e_i - 1}\left(p_i - 1\right)\right\}$$

To begin, we substitute $N = \prod_i \{p_i^{e_i}\}$ for N in the previous expression. This gives

$$\phi(N) = \phi\left(\prod_i \{p_i^{e_i}\}\right)$$

Using the result $\phi(pq) = \phi(p)\ \phi(q)$, we have

$$\phi(N) = \prod_i \{\phi(p_i^{e_i})\}$$

Finally, we apply the result $\phi(p^e) = p^{e-1}(p-1)$ to obtain

$$\phi(N) = \prod_i \left\{p_i^{e_i-1}(p_i-1)\right\}$$

as expected.