

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

$$\mathbb{Z}_{p^e}^* \subset \{1, 2, \dots, p^e - 1\} \quad (3.1)$$

This implies the following relation between the cardinalities of these sets

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

where $|\{1, 2, \dots, p^e - 1\}|$ has the value $|\{1, 2, \dots, p^e - 1\}| = (p^e - 1)$. It follows that the value of $|\mathbb{Z}_{p^e}^*|$ can be obtained by determining the set of all values in $\{1, 2, \dots, p^e - 1\}$ that do not satisfy the condition 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 p . Thus, the set of values in $\{1, 2, \dots, p^e - 1\}$ that do not satisfy the condition in 3.1 may be defined as

$$\{p, 2p, 3p, \dots, p, 2p, 3p, \dots, p^2 p, \dots, (p^{e-1} - 1)p\}$$

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

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

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

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

as desired.

To show that

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

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}^* is $pq - 1$. As before, we must take into account that some possible elements of \mathbb{Z}_{pq}^* will not satisfy the definition in 3.1. If we subtract the number of these elements, then we will have $\phi(pq) = |\mathbb{Z}_{pq}^*|$. 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

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

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

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

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

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

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

as expected.