<u>Problem 5):</u> First, we will show that if $x \in \mathbb{Z}_N$, then $\forall x \in \mathbb{Z}_N^\star$, $f(x) = (x_p, x_q)$ where $x_p \in \mathbb{Z}_p$ & $x_q \in \mathbb{Z}_q$ and $x_p \in \mathbb{Z}_p^\star$ & $x_q \in \mathbb{Z}_q^\star$. To do this, we assume, to the contrary, that $x_p \notin \mathbb{Z}_p^\star$. This assumption implies that $\gcd([x \mod p], p) \neq 1$ and, by extension, that $\gcd(x, p) \neq 1$. Moreover, this leads to the conclusion that $\gcd(x, N) \neq 1$. This cannot be, otherwise we would have $z \notin \mathbb{Z}_N^\star$, violating the definition of $\mathbb{Z}_N^\star$ we started with. Therefore, $x_p \in \mathbb{Z}_p^\star$ *must* hold. To show that $x_q \in \mathbb{Z}_q^\star$ *must* also hold, we make the similar contrary assumption (that $x_q \notin \mathbb{Z}_q^\star$) and arrive at a similar contradiction, thereby requiring that $x_q \in \mathbb{Z}_q^\star$.

Next, we will show that f is an isomorphism. We begin by showing that f is <u>one-to-one</u>. To begin, let

$$f(x) = (x_p, x_q) = f(x')$$

Then, we let

$$x = x_p = x' \mod p$$

and

$$x = x_q = x' \mod q$$

This implies that $(x - x')$ is divisible by both p and q. However, since $p|N$ & $q|N$ and $\gcd(p, q) = 1$, we must have $(x - x')$ divisible by $pq = N$. This implies that $x = x' \mod N$ and $x' = x \mod N$. Moreover, since $x, x' \in \mathbb{Z}_N$, we <u>must</u> have $x = x'$ so f *must* alsp be **one-to-one**.

Continuing, since $|\mathbb{Z}_p| = p$ and $|\mathbb{Z}_q| = q$, we must have

$$|\mathbb{Z}_p \times \mathbb{Z}_q| = |\mathbb{Z}_p| \cdot |\mathbb{Z}_q| = pq \tag{5.1}$$

Now, we have $N = pq$ and $|\mathbb{Z}_N| = N$, so the expression in 5.1 becomes

$$\begin{aligned} |\mathbb{Z}_p \times \mathbb{Z}_q| &= pq \\ &= N \\ &= |\mathbb{Z}_N| \end{aligned}$$

Therefore, f must also be onto and, by extension, bijective.

Finally, we must show that

$$\begin{aligned} f\left((a+b) \mod N\right) &= [(a+b) \mod p] \circ_{\mathbb{Z}_N} [(a+b) \mod q] \\ &= [(a+b) \mod p] \boxplus [(a+b) \mod q] \\ &= f(a) \boxplus f(b) \end{aligned}$$

Since we have defined $f(x) \equiv ([x \mod p], [x \mod q])$, we may write $f\left((a+b) \mod N\right)$ as

$$f\left((a+b) \mod N\right) = \left([[(a+b) \mod N] \mod p], [[(a+b) \mod N] \mod q]\right) \tag{5.2}$$

Now, since $p|N$ and $q|N$, we have

$$\begin{aligned} [[X \mod N] \mod p] &= [[X \mod p] \mod p] \\ &= [X \mod p] \end{aligned}$$

and

$$\begin{aligned}[[X \mod N] \mod q] &= [[X \mod q] \mod q] \\ &= [X \mod p]\end{aligned}$$

Therefore, the expression in 5.2 becomes

$$\begin{aligned}f\left((a+b) \mod N\right) &= \left([[(a+b) \mod N] \mod p], [[(a+b) \mod N] \mod q]\right) \\ &= \left([[(a+b) \mod p] \mod p], [[(a+b) \mod q] \mod q]\right) \\ &= \left([(a+b) \mod p], [(a+b) \mod q]\right)\end{aligned}$$

Separating this result according to a and b gives

$$\begin{aligned}\left([(a+b) \mod p], [(a+b) \mod q]\right) &= \left([a \mod p], [a \mod q]\right) \boxplus \left([b \mod p], [b \mod q]\right) \\ &= f(a) \boxplus f(b)\end{aligned}$$

as desired.

□