

Problem 5): First, we will show that if $x \in \mathbb{Z}_N$, then $\forall x \in \mathbb{Z}_N^*$, $f(x) = (x_p, x_q)$ where $x_p \in \mathbb{Z}_p$ & $x_q \in \mathbb{Z}_q$ and $x_p \in \mathbb{Z}_p^*$ & $x_q \in \mathbb{Z}_q^*$. To do this, we assume, to the contrary, that $x_p \notin \mathbb{Z}_p^*$. This assumption implies that $\gcd([x \bmod p], p) \neq 1$ 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 $x \notin \mathbb{Z}_N^*$, violating the definition of \mathbb{Z}_N^* we started with. Therefore, $x_p \in \mathbb{Z}_p^*$ *must* hold. To show that $x_q \in \mathbb{Z}_q^*$ *must* also hold, we make the similar contrary assumption (that $x_q \notin \mathbb{Z}_q^*$) and arrive at a similar contradiction, thereby requiring that $x_q \in \mathbb{Z}_q^*$.

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

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

Then, we let

$$x = x_p = x' \bmod p$$

and

$$x = x_q = x' \bmod q$$

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 $x = x' \bmod N$ and $x' = x \bmod N$. Moreover, since $x, x' \in \mathbb{Z}_N$, we must have $x = x'$ so f *must* also 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

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

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

$$f((a+b) \bmod N) = ([[(a+b) \bmod N] \bmod p], [[(a+b) \bmod N] \bmod q]) \quad (5.2)$$

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

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

and

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

Therefore, the expression in 5.2 becomes

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

Separating this result according to a and b gives

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

as desired.

□