Problem 1): Let $x, y, e, x^{-1} \in \mathcal{G}$ where $e \in \mathcal{G}$ is the identity element of $\mathcal{G}$ and x^{-1} is such that both $x\,x^{-1} = e = x^{-1}\,x$ and $y\,x^{-1} = e = x^{-1}\,y$ hold. Therefore we have

$$x\,x^{-1} = y\,x^{-1} \tag{1.1}$$

$$x\,x^{-1} = x^{-1}\,y \tag{1.2}$$

$$x^{-1}\,x = y\,x^{-1} \tag{1.3}$$

$$x^{-1}\,x = x^{-1}\,y \tag{1.4}$$

By applying the cancelation rule ($ab = ac \;\Rightarrow\; b = c$ for $a, b, c \in \mathbb{G}$ for any group $\mathbb{G}$) to the expression in 1.1 and 1.4, it is clear that we have

$$x = y \tag{1.5}$$

Since $\mathcal{G}$ is abelian, we may rewrite the expression in 1.2 as

$$x\,x^{-1} = x^{-1}\,x = x^{-1}\,y$$

or

$$x\,x^{-1} = y\,x^{-1} = x^{-1}\,y$$

From either expression, the application of the cancelation rule yields the same result as in expression 1.5. Similarly, we use the abelian property of $\mathcal{G}$ to rewrite the expression in 1.3 as

$$x^{-1}\,x = x\,x^{-1} = y\,x^{-1}$$

or

$$x^{-1}\,x = x^{-1}\,y = y\,x^{-1}$$

Again, applying the cancelation rule to either expression yields the same result as in 1.5. Therefore, every element in an abelian group must have a unique inverse.

□

Problem 2): Let $\mathcal{G}$ be a finite group and $g \in \mathcal{G}$. Now define $\langle g \rangle \equiv g^0, g^1, g^2, \ldots, g^k, \ldots$, where $k \in \mathbb{N}$. Beginning with the multiplicative case, let $m, n \in \mathbb{N}$ so that we have

$$g^m\,g^n = g^{m+n}$$

Since $m, n \in \mathbb{N}$ and $\mathbb{N}$ is closed under addition, $(m+n) \in \mathbb{N}$, it is clear that $g^{m+n} \in \langle g \rangle$. Therefore, $\langle g \rangle$ is closed under its operation. From our definition of $\langle g \rangle$, we know that $g^0 \in \langle g \rangle$. Additionally, $g^0 \equiv e = 1$; therefore $\langle g \rangle$ contains the identity element. Now, let $m \in \mathbb{Z}^+$ and write $g^{-m}\,g^m$. Using $g^{-m} \equiv \left(g^{-1}\right)^m$, this yields

$$g^{-m}\,g^m = \left(g^{-1}\right)^m\,g^m = \left(g^{-1}\,g\right)^m = (e)^m = e = 1$$

which implies the existence of an inverse for each element in $\langle g \rangle$. Finally, let $m, n, k \in \mathbb{N}$, then we have

$$g^m\,\left(g^n\,g^k\right) = g^m\,\left(g^{n+k}\right) = g^{m+(n+k)} \tag{2.1}$$

Since $\mathbb{N}$ is associative under addition, the expression in 2.1 may be rewritten as

$$g^{m+(n+k)} = g^{(m+n)+k} = \left(g^{m+n}\right)\,g^k = \left(g^m\,g^n\right)\,g^k$$

thereby demonstrating the associativity of operations in $\langle g \rangle$. Since $\mathcal{G}$ is finite, it has order $m = |\mathcal{G}|$. Therefore, the elements of $\langle g \rangle$ will be repeats of elements in $\mathcal{G}$ starting with g^{m+1}. Moreover, this means that $\langle g \rangle \subseteq \mathcal{G}$, thus satisfying the last condition for $\langle g \rangle$ to be a sub-group of $\mathcal{G}$.

Continuing with the additive case, let $m, n \in \mathbb{N}$ so that we have

$$m \times g\, n \times g = (m+n) \times g$$

Since $m, n \in \mathbb{N}$ and $\mathbb{N}$ is closed under addition, $(m+n) \in \mathbb{N}$, it is clear that $(m+n) \times g \in \langle g \rangle$. Therefore, $\langle g \rangle$ is closed under its operation. From our definition of $\langle g \rangle$, we know that $0 \times g \in \langle g \rangle$. Additionally, $0 \times g \equiv e = 0$; therefore $\langle g \rangle$ contains the identity element. Now, let $m \in \mathbb{Z}^+$ and write $(-m) \times g\, m \times g$. Using $(-m) \times g \equiv m \times (-g)^m$, this yields

$$(-m) \times g\, m \times g = m \times (-g)\ m \times g = m \times (-g\, g) = m \times (e) = e = 0$$

which implies the existence of an inverse for each element in $\langle g \rangle$. Finally, let $m, n, k \in \mathbb{N}$, then we have

$$m \times g\ (n \times g\, k \times g) = m \times g\ ((n+k) \times g) = (m + (n+k)) \times g \tag{2.2}$$

Since $\mathbb{N}$ is associative under addition, the expression in 2.2 may be rewritten as

$$(m + (n+k)) \times g = ((m+n)+k) \times g = (m+n) \times g\, k \times g = (m \times g\, n \times g)\ k \times g$$

thereby demonstrating the associativity of operations in $\langle g \rangle$. Since $\mathcal{G}$ is finite, it has order $m = |\mathcal{G}|$. Therefore, the elements of $\langle g \rangle$ will be repeats of elements in $\mathcal{G}$ starting with $(m+1) \times g$. Moreover, this means that $\langle g \rangle \subseteq \mathcal{G}$, thus satisfying the last condition for $\langle g \rangle$ to be a sub-group of $\mathcal{G}$.

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

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

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 $\mathbb{Z}_{pq}^{\star}$ 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 $\phi(pq) = |\mathbb{Z}_{pq}^{\star}|$. 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

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

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

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

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

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

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

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

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

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

as expected.

Problem 4): We denote the cross product of groups $\mathcal{G}$ and $\mathcal{H}$ as $\mathcal{G}\times\mathcal{H}$ and define it by

$$(g,h)\circ(g',h')\equiv(g\circ_{\mathcal{G}}g'\ ,\ h\circ_{\mathcal{H}}h') \tag{4.1}$$

To show that $\mathcal{G}\times\mathcal{H}$ is a group, we begin by proving closure under its operation. Since $\mathcal{G}$ and $\mathcal{H}$ are groups, the we have $(g\circ_{\mathcal{G}}g')\in\mathcal{G}$ and $(h\circ_{\mathcal{H}}h')\in\langle$. Thus $\mathcal{G}\times\mathcal{H}$ is closed under its operation. Next, we must show the existence of an identity in $\mathcal{G}\times\mathcal{H}$. If we modify the expression in 4.1 so that $g'=e_{\mathcal{G}}$ and $h'=e_{\mathcal{H}}$, then we have

$$\begin{aligned}(g,h)\circ(e_{\mathcal{G}},e_{\mathcal{H}})&=(g\circ_{\mathcal{G}}e_{\mathcal{G}}\ ,\ h\circ_{\mathcal{H}}e_{\mathcal{H}})\\&=(g,h)\end{aligned}$$

Therefore, $\mathcal{G}\times\mathcal{H}$ contains an identity element and it is defined as $(e_{\mathcal{G}},e_{\mathcal{H}})$. Next, we must demonstrate the existence of inversed in $\mathcal{G} \times \mathcal{H}$. To do this, we again modify the expression in 4.1. This time we substitute $g' = g^{-1}$ and $h' = h^{-1}$. Applying this substitution to the expression in 4.1 gives

$$\begin{aligned}(g, h) \circ \left(g^{-1}, h^{-1}\right) &= \left(g \circ_{\mathcal{G}} g^{-1}\ ,\ h \circ_{\mathcal{H}} h^{-1}\right) \\ &= \left(e_{\mathcal{G}}, e_{\mathcal{H}}\right)\end{aligned}$$

Thus, $\mathcal{G} \times \mathcal{H}$ contains inverses for each of its elements. Lastly, we show that associativity holds in $\mathcal{G} \times \mathcal{H}$. We begin with

$$\begin{aligned}((g_1, h_1) \circ (g_2, h_2)) \circ (g_3, h_3) &= (g_1 \circ_{\mathcal{G}} g_2, h_1 \circ_{\mathcal{H}} h_2) \circ (g_3, h_3) \\ &= ((g_1 \circ_{\mathcal{G}} g_2) \circ_{\mathcal{G}} g_3, (h_1 \circ_{\mathcal{H}} h_2) \circ_{\mathcal{H}} h_3) \qquad (4.2)\end{aligned}$$

Using the associativity of $\mathcal{G}$ and $\mathcal{H}$, we have

$$((g_1 \circ_{\mathcal{G}} g_2) \circ_{\mathcal{G}} g_3, (h_1 \circ_{\mathcal{H}} h_2) \circ_{\mathcal{H}} h_3) = (g_1 \circ_{\mathcal{G}} (g_2 \circ_{\mathcal{G}} g_3), h_1 \circ_{\mathcal{H}} (h_2 \circ_{\mathcal{H}} h_3))$$

Thus, the expression in 4.2 becomes

$$\begin{aligned}((g_1, h_1) \circ (g_2, h_2)) \circ (g_3, h_3) &= ((g_1 \circ_{\mathcal{G}} g_2) \circ_{\mathcal{G}} g_3, (h_1 \circ_{\mathcal{H}} h_2) \circ_{\mathcal{H}} h_3) \\ &= (g_1 \circ_{\mathcal{G}} (g_2 \circ_{\mathcal{G}} g_3), h_1 \circ_{\mathcal{H}} (h_2 \circ_{\mathcal{H}} h_3))\end{aligned}$$

which implies that associativity holds for $\mathcal{G} \times \mathcal{H}$.

□

Problem 5): 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 one-to-one. 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 must 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 <u>onto</u> and, by extension, <u>bijective</u>.

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 $f((a+b) \mod N)$ 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

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

Separating this result according to a and b gives

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

as desired.

□

Problem 6): We begin by applying the function mapping $\mathbb{Z}_N$ to $\mathbb{Z}_p \times \mathbb{Z}_q$ (denoted f) to $(x^e)^d$. This gives us

$$\begin{aligned} f\left((x^e)^d\right) &= \left(\left[\left(x_p^e\right)^d \mod p\right], \left[\left(x_q^e\right)^d \mod q\right]\right) \\ &= \left(\left[\left(x_p^{e\,d}\right) \mod p\right], \left[\left(x_q^{e\,d}\right) \mod q\right]\right) \end{aligned}$$

We now substitute $ed = 1 \mod \phi(N)$ into our previous result to obtain

$$\begin{aligned} f\left((x^e)^d\right) &= \left(\left[\left(x_p^{e\,d}\right) \mod p\right], \left[\left(x_q^{e\,d}\right) \mod q\right]\right) \\ &= \left(\left[\left(x_p^{1 \mod \phi(N)}\right) \mod p\right], \left[\left(x_q^{1 \mod \phi(N)}\right) \mod q\right]\right) \end{aligned}$$

Using the definition of $\phi(\cdots)$ as well as the fact that $N = pq$, where p and q are distinct primes, we note that $\phi(N) = \phi(p)\,\phi(q)$. Therefore, our previous result can be rewritten as

$$
\begin{aligned}
f\left((x^e)^d\right) &= \left(\left[\left(x_p^{1 \mod \phi(N)}\right) \mod p\right], \left[\left(x_q^{1 \mod \phi(N)}\right) \mod q\right]\right) \\
&= \left(\left[\left(x_p^{1 \mod \phi(p)\,\phi(q)}\right) \mod p\right], \left[\left(x_q^{1 \mod \phi(p)\,\phi(q)}\right) \mod q\right]\right) \qquad (6.1)
\end{aligned}
$$

Using the relation $a^{\phi(N)} = 1 \mod N$, we see that $\phi(q)$ will cancel from the exponent in the first part of the left-hand-term in 6.1. Similarly, $\phi(q)$ will also cancel from the second part of the left-hand-term in 6.1. Therefore, our expression in 6.1 can be simplified to give

$$
\begin{aligned}
f\left((x^e)^d\right) &= \left(\left[\left(x_p^{1 \mod \phi(p)\,\phi(q)}\right) \mod p\right], \left[\left(x_q^{1 \mod \phi(p)\,\phi(q)}\right) \mod q\right]\right) \\
&= \left(\left[\left(x_p^{1 \mod \phi(q)}\right) \mod p\right], \left[\left(q^{1 \mod \phi(p)}\right) \mod q\right]\right)
\end{aligned}
$$

Noting that $b \mod p = [b \mod c] \mod c$, we modify our previous result to give

$$
\begin{aligned}
f\left((x^e)^d\right) &= \left(\left[\left(x_p^{1 \mod \phi(q)}\right) \mod p\right], \left[\left(x_q^{1 \mod \phi(p)}\right) \mod q\right]\right) \\
&= \left(\left[\left(\left(x_p^{1 \mod \phi(q)}\right) \mod p\right) \mod p\right], \left[\left(\left(x_q^{1 \mod \phi(p)}\right) \mod q\right) \mod q\right]\right)
\end{aligned}
$$

Again using the relation $a^{\phi(N)} = 1 \mod N$, we are able to simplify our previous result as

$$
\begin{aligned}
f\left((x^e)^d\right) &= \left(\left[\left(\left(x^{1 \mod \phi(q)}\right) \mod p\right) \mod p\right], \left[\left(\left(x^{1 \mod \phi(p)}\right) \mod q\right) \mod q\right]\right) \\
&= \left(\left[\left(x_p \mod (pq)\right) \mod p\right], \left[\left(x_q \mod (qp)\right) \mod q\right]\right) \qquad (6.2)
\end{aligned}
$$

Finally, we note that $pq = qp = N$ and recall the definition of $f(\cdots)$. These relations allow us to rewrite our result in expression 6.2 to give

$$
\begin{aligned}
f\left(\left(x^e\right)^d\right) &= \left(\left[\left(x_p \mod (pq)\right) \mod p\right], \left[\left(x_q \mod (qp)\right) \mod q\right]\right) \\
&= \left(\left[\left(x_p \mod N\right) \mod p\right], \left[\left(x_q \mod N\right) \mod q\right]\right) \\
&= f\left(x \mod N\right)
\end{aligned}
$$

We then take the inverse of $f(\cdots)$ to ultimately give

$$
f\left(\left(x^e\right)^d\right) = f\left(x \mod N\right) \implies \left(x^e\right)^d = x \mod N
$$

as desired.

□

Problem 7): We start with $a^{\phi(N)} = 1 \mod N$ and note $\phi(N) = \phi(p)\,\phi(q)$ to obtain

$$
a^{\phi(N)} = 1 \mod N = a^{\phi(p)\,\phi(q)}
$$

Since $\phi(p) = p - 1$ and $\phi(q) = q - 1$, the previous result is equivalent to

$$
\begin{aligned}
a^{\phi(N)} = 1 &\mod N = a^{\phi(p)\,\phi(q)} \\
1 &\mod N = a^{(p-1)(q-1)}
\end{aligned}
$$

$a^{p-1} = 1 \mod p$, and $a^{q-1} = 1 \mod q$

Problem 8):

Problem 9):

Problem 10):

Problem 11):

Problem 12):

Problem 14):

Problem 15):

Problem 16):

Problem 17):

Problem 18):