

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

$$x x^{-1} = y x^{-1} \quad (1.1)$$

$$x x^{-1} = x^{-1} y \quad (1.2)$$

$$x^{-1} x = y x^{-1} \quad (1.3)$$

$$x^{-1} x = x^{-1} y \quad (1.4)$$

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

$$x = y \quad (1.5)$$

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 $\langle g \rangle \equiv g^0, g^1, g^2, \dots, g^k, \dots$, 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 $g^{-m} \equiv (g^{-1})^m$, this yields

$$g^{-m} g^m = (g^{-1})^m g^m = (g^{-1} g)^m = (e)^m = e = 1$$

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

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

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

$$g^{m+(n+k)} = g^{(m+n)+k} = (g^{m+n}) g^k = (g^m g^n) g^k$$

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

$$m \times g (n \times g k \times g) = m \times g ((n + k) \times g) = (m + (n + k)) \times g \quad (2.2)$$

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 $\mathbb{Z}_p^* \equiv \{a \in \{1, 2, \dots, p-1\} \mid \gcd(a, p) = 1\}$, 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

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

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

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

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.

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

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

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, then we have $(g \circ_{\mathcal{G}} g') \in \mathcal{G}$ and $(h \circ_{\mathcal{H}} h') \in \mathcal{H}$. 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 inverses 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

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

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

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

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 $\forall x \in \mathbb{Z}_N^*$, $f(x) = (x_p, x_q)$ 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 $z \notin \mathbb{Z}_N^*$, 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

$$x = x_p = x' \pmod{p}$$

and

$$x = x_q = x' \pmod{q}$$

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 $x = x' \pmod{N}$ and $x' = x \pmod{N}$. 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

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

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.

□

Problem 6): We begin by substituting $ed = 1 \bmod \phi(N)$ into $(x^e)^d = x^{ed}$ to obtain

$$\begin{aligned}
 \phi\left((x^e)^d\right) &= \phi(x \bmod N) \\
 &=
 \end{aligned}$$

Problem 7):

Problem 8):

Problem 9):

Problem 10):

Problem 11):

Problem 12):

Problem 14):

Problem 15):

Problem 16):

Problem 17):

Problem 18):