

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 we have $\phi(p^e) = |\mathbb{Z}_{p^e}^*|$, by the definitions of $\phi(p)$ and \mathbb{Z}_p^* for any prime p ,

$$\phi(p^e) = |\mathbb{Z}_{p^e}^*|$$