Definition 1 (Left Coset)**.** Let G be a group and H be a subgroup of G. Left coset of H with representative $g \in G$ is the set

$$gH = \{gh : h \in H\}$$

Definition 2 (Right Coset)**.** Let G be a group and H be a subgroup of G. Right coset of H with representative $g \in G$ is the set

$$Hg = \{hg : h \in H\}$$

Example 1 (Cosets)**.** Let H be the subgroup of $\mathbb{Z}_6$ consisting of the elements $\{0, 3\}$. The cosets are

$$\begin{aligned} 0 + H = 3 + H = \{0, 3\} \\ 1 + H = 4 + H = \{1, 4\} \\ 2 + H = 5 + H = \{2, 5\} \end{aligned}$$

Definition 3 (Index of a subgroup)**.** Let G be a group and H be a subgroup of G. The index $[G : H]$ of H in G is the number of left cosets of H in G.

Example 2 (Index of a subgroup)**.** Let $G = \mathbb{Z}_6$ and $H = \{0, 3\}$. Then $[G : H] = 3$.

Theorem 1. Let H be a subgroup of a group G. Then the left (same as right) cosets of H in G partition G. That is, the group G is the disjoint union of the left (same as right) cosets of H in G.

Proof. Let g_1H and g_2H be two cosets of H in G. We must show that either $g_1H \cap g_2H = \emptyset$ or $g_1H = g_2H$. Suppose that $g_1H \cap g_2H \neq \emptyset$ and $a \in g_1H \cap g_2H$. Then by definition of a left coset, $a = g_1h_1 = g_2h_2$ for some elements $h_1, h_2 \in H$.

Let $x \in g_1H$. Then there exists $h_k \in H$ such that $x = g_1h_k$. Then

$$x = g_1h_k = g_1h_1h_1^{-1}h_k = g_2h_2h_1^{-1}h_k \in g_2H \ ,$$

and therefore $g_1H \subseteq g_2H$.

Let $y \in g_2H$. Then there exists $h_m \in H$ such that $x = g_2h_m$. Then

$$x = g_2h_m = g_2h_2h_2^{-1}h_m = g_1h_1h_2^{-1}h_m \in g_1H \ ,$$

and therefore $g_2H \subseteq g_1H$. Therefore, $g_1H = g_2H$. □

Theorem 2. Let H be a subgroup of G with $g \in G$. The number of elements in H is the same as the number of elements in gH.

Proof. Let $\phi : H \to gH$ be defined by $h \mapsto gh$. Define an inverse mapping $\psi : gH \to H$ by $a \mapsto g^{-1}a$. First we show that ψ is well defined. Since $a \in gH$, then $a = gh$ for some $h \in H$. $g^{-1}a = g^{-1}gh = h \in H$. We show that ϕ is a bijection.

$$\begin{aligned} (\phi \circ \psi)(a) = \phi(g^{-1}a) = gg^{-1}a = a \ , \\ (\psi \circ \phi)(h) = \psi(gH) = g^{-1}gh = h \ . \end{aligned}$$

Therefore, ϕ is a bijection between H and gH. Hence, the number of elements in H is the same as the number of elements in gH. □

Theorem 3 (Lagrange)**.** Let G be a finite group and let H be a subgroup of G. Then $|G|/|H| = [G:H]$ is the number of distinct left cosets of H in G. In particular, the number of elements in H must divide the number of elements in G.

Proof. Every subgroup $H \subseteq G$ partitions G into $[G:H]$ distinct left cosets. Each left coset has $|H|$ elements, therefore, $|G| = [G:H]|H|$. $\square$

Theorem 4. Every Carmichael number n is odd.

Proof. Let n be a Carmichael number. Since n is composite, we conclude $n \geqslant 4$. Since $n-1$ is relatively prime to n, $(n-1)^{n-1} \equiv 1 \pmod{n}$, so $(-1)^{n-1} \equiv 1 \pmod{n}$, and we know $(-1)^{n-1} = \pm 1$. Since $n > 2$, it holds that $-1 \not\equiv 1 \pmod{n}$, so $(-1)^{n-1} = 1$. Thus $n-1$ is even, which implies n is odd. $\square$