LAGRANGE'S THEOREM – ANSWER

Notation: The number of elements in a group (or set) *G*, also called the order of *G*, is denoted by $|G|$.

Theorem: If *H* is a subgroup of a finite group *G*, then the order of *H* is a divisor of the order of *G*.

Proof: Suppose that *H* is a subgroup of a finite group *G*, and suppose that $|G| = n$ and $|H| = m$. If $H = G$, then clearly $m = n$ and, thus, *m* divides *n*. Hence, suppose that $H \neq G$. Then there exists $a \in G$ such that $a \notin H$, and by previous proof, $|H| = |Ha|$ and $H \cap Ha = \varnothing$. Continuing in this manner, if $H \cup Ha \neq G$, then there exists $b \in G$ such that $b \notin H$ and $|H| = |Ha| = |Hb|$ and no two of these right cosets have any elements in common. If now $H \cup Ha \cup Hb \neq G$, then we can continue in this manner, but since *G* is a finite group, we will eventually arrive at a set of right cosets whose union is *G*. Furthermore, since these cosets all contain *m* elements and since no two cosets have any elements in common, if we have exactly *k* such right cosets whose union is *G*, then the number of elements in *G* is equal to the number of elements in *H* times the number of distinct right cosets of *H* in *G*. In other words, $n = mk$ and, therefore, $m = |H|$ is a divisor of $n = |G|$.

□