In this tutorial we will be looking at cyclic groups and subgroups. Let G be a group with identity e. Recall that for $x \in G$ and $n \in \mathbb{Z}$, we define x^n by declaring that $x^0 = e$, $x^{n+1} = xx^n$, and for $n > 0$, $x^{-n} = (x^{-1})^n$. You may assume that $x^m x^n = x^{m+n}$ and $(x^m)^n = x^{mn}$ for all $m, n \in \mathbb{Z}$.

1. Prove that if $n \in \mathbb{Z}$, $k \in \mathbb{N}$ then $x^n = x^{n+k}$ iff $x^k = e$.

2. Suppose G is finite. Show that for each $x \in G$ there is some $k \in \mathbb{N}$ with $x^k = e$. We call the least such k the *order* of x, $o(x)$.

3. Show that for any group G and any $x \in G$ the set $\langle x \rangle = \{ x^n : n \in \mathbb{Z} \}$ is a subgroup of G.

4. Suppose that $x^n = e$ for some $n \in \mathbb{N}$. Show that $o(x) \mid n$. [Hint: divide $o(x)$ into n using the division algorithm.]

5. Show that if G is finite and $x \in G$ then $| \langle x \rangle | = o(x)$. Deduce that $o(x) \mid o(G)$ for all $x \in G$, where $o(G)$ denotes the number of elements of G.

Note: we call a group G *cyclic* if there is some x such that $G = \langle x \rangle$. We call such an x a *generator* for G. Note that every cyclic group is abelian because $x^m x^n = x^{m+n} = x^{n+m} = x^n x^m$.