3. State and prove Lagrange's Theorem. If H is a subgroup of the finite group G, then the order of H divides the order of G.

Proof

Step 1 I claim that every element of G is in exactly one right coset of H in G. Surely $g \in Hg$. If g is also in Hg', then $g = h'g'$ for some $h' \in H$. I will show $Hg = Hg'$.

$\subseteq$ Take $hg \in Hg$ for some $h \in H$. Observe that $hg = hh'g' \in Hg'$.

$\supseteq$ Take $hg' \in Hg'$ for some $h \in H$. Observe $hg' = h(h')^{-1}g \in Hg$.

Thus $Hg = Hg'$ as claimed.

At this point we may pick r elements $g_1, \ldots, g_r$ in G such that every element of G is in exactly one of the cosets $Hg_1, \ldots, Hg_r$.

Step 2 Every coset Hg has the same number of elements as H.

Pf consider $\varphi: H \to Hg$, given by $\varphi(h) = hg$. φ is onto because a typical element of Hg is hg for some $h \in H$ and $\varphi(h) = hg$. φ is one-to-one because if h and $h' \in H$ with $\varphi(h) = \varphi(h')$, then $hg = h'g$ so multiplying by g^{-1} to learn $h = h'$.

Now we have

Order of G = (the # of cosets)(the # of elements in each coset)

$\therefore$ order of $G = r$ (order of H) ☒

4. Prove that every subgroup of $(\mathbb{Z}, +)$ is cyclic. I want a complete proof. "We did this in class" and "This follows from a Theorem we proved in class" are not good enough.

Let H be a subgroup of $\mathbb{Z}$. If $H = \{0\}$ H is cyclic. Otherwise it has some positive elements in it. Let h be the smallest positive element in H. I will prove that $H = \langle h \rangle$.

It is clear that $\langle h \rangle \subseteq H$.

I now show $H \subseteq \langle h \rangle$. Take h', an arbitrary element of H. Divide to see that $h' = qh + r$ for some integers q and r with $0 \leq r \leq h - 1$.

$h' - qh = r$ is in H. Thus $r = 0$, $h' = qh \in \langle h \rangle$ and H is the cyclic group $\langle h \rangle$.