48

3. Let m and n be positive integers. Let H be the set of all linear combinations $an + bm$, where a and b are integers. It can be shown that there exists a positive element $h \in H$, so that every element of H is a multiple of h. PROVE that h is the greatest common divisor of m and n. (I am not asking you to prove the existence of h. I am saying, "Suppose h exists. Now prove that h is the g.c.d.".) Let $d = g.c.d\ (m,n)$.

$h \in H$ so $h = an + bm$ for some a and $b \in \mathbb{Z}$. We know $d|n$ and $d|m$ so d also $|\, h$.
On the other hand, $n \in H$ so $h|n$ and $m \in H$ so $h|m$. Thus h is a common divisor of n and m. But d is the greatest common divisor of m and n. Thus $h \leq d$ and $d|h$, with d and h positive. This is possible only if $d = h$.

4. Give an example of a group G and elements a and b in G of finite order with the order of ab not equal to the order of a times the order of b.

$G = S_3$ $\quad a = (12)$ $\quad b = (13)$ $\quad ab = (12)(13) = (132)$

a and b have order 2 but ab has order 3.