76

4. DEFINE *normal subgroup.* The subgroup N of the group G is normal if $gng^{-1} \in N$ for all $n \in N$ and $g \in G$.

5. STATE Lagrange's Theorem. If H is a subgroup of the finite group G, then the order of H divides the order of G.

Proof Consider the right cosets of H in G. Every element of G is in exactly one right coset because if two cosets have any element in common, then the two cosets are equal. Each coset has the same number of elements as H because $f: H \to Hx$, given by $f(h) = hx$ is a one-to-one and onto function. So G consists of r cosets and each coset has $|H|$ elements. Thus $|G| = r|H|$.

6. STATE the lemma from number theory about linear combinations and greatest common divisors.

Let d be the greatest common divisor of the integers m and n. Then there exists integers r and s with $d = rm + sn$.

Proof Let $H = \{rm + sn \mid r, s \in \mathbb{Z}\}$. Observe that H is a subgroup of $\mathbb{Z}$. Every subgroup of $\mathbb{Z}$ is cyclic so $H = \langle h \rangle$ for some $h \in H$. I will show that $h = d$. On the one hand, $h \in H$ so $h = rm + sn$ for some integers $r, s \in \mathbb{Z}$. We see that $d \mid m$ and $d \mid n$ so $d \mid h$. On the other hand, $m, n \in H = \langle h \rangle$. So $h \mid m$ and $h \mid n$. But d is the greatest common divisor of m and n so $h \mid d$. We have d and h positive integers with $d \mid h$ and $h \mid d$. Thus $d = h$.