Let \( p \) be an integer satisfying: whenever \( p | mn \), then \( p | m \) or \( p | n \). Then \( p \) is a prime.

**Proof.** Suppose that \( p \) is not a prime and \( p \) satisfies the condition above. Then \( p = rs \) with \( r, s > 1 \) and thus \( r, s < p \). Now \( p | rs \) and since \( r, s < p \), it follows that \( p \) \( \not| \) \( r \) and \( p \) \( \not| \) \( s \), a contradiction. Therefore \( p \) is a prime.

Assume that \( d = sa + tb \), all integers. Find infinitely many pairs of integers, \((s_k, t_k)\) such that \( d = s_k a + t_k b \).

**Proof.** Let \( s_k = s + kb \) and \( t_k = t - ka \), for all positive integers \( k \). Then \( s_k a + t_k b = (s + kb)a + (t - ka)b = sa + kba + tb - kab = sa + tb = d \).

Show that the integer \( M > 0 \) is the lcm of \( a_1, a_2, \ldots, a_n \) if and only if it is a common multiple of \( a_1, a_2, \ldots, a_n \) which divides every other common multiple.

**Proof.** Suppose that \( M \) is the lcm of \( a_1, a_2, \ldots, a_n \) and that \( N \) is another common multiple. Then by the division algorithm, \( N = Mq + r \) with \( 0 \leq r < M \). Thus \( a_i | N \) and \( a_i | M \) for all \( i \) and therefore \( a_i | r \) for all \( i \). Hence \( r \) is a common multiple of \( a_1, a_2, \ldots, a_n \) and \( r < M \) which is the LEAST common multiple. Therefore \( r = 0 \) and so \( M \) is a divisor of \( N \).

Now assume that \( M \) is a common multiple of \( a_1, a_2, \ldots, a_n \) which divides every other common multiple. Then \( M \) is smaller than every other common multiple and hence is the lcm.

(i) Show that \( \alpha^r = 1 \) if \( \alpha \) is an \( r \)-cycle.

(ii) Show that \( r \) is the smallest positive integer satisfying \( \alpha^r = 1 \) for the \( r \)-cycle \( \alpha \).

**Proof.** (i) Let \( \alpha \) be described as in the definition on Page 99. Then \( \alpha^j(i_r) = i_{r+j} \) with \( r + j \) reduced modulo \( r \) when \( i + j > r \). Then \( \alpha^r(i_s) = i_{s+r} = i_s \) for all \( s \). Thus \( \alpha^r = 1 \).

(ii) \( \alpha^k(i_1) = i_{1+k} \) ands if \( k < r \), \( i_{1+k} \neq i_1 \). Thus \( \alpha^k \neq 1 \).

(i) Prove that if \( \alpha \) and \( \beta \) are commuting permutations, then \( (\alpha \cdot \beta)^k = \alpha^k \cdot \beta^k \).

(ii) Find 2 permutations \( \alpha \) and \( \beta \) such that \( (\alpha \cdot \beta)^2 \neq \alpha^2 \cdot \beta^2 \).

**Proof.** (i) \((\alpha \cdot \beta)^k = (\alpha \cdot \beta) \cdot (\alpha \cdot \beta) \ldots (\alpha \cdot \beta) \) \( k \) times. Since \( \alpha \cdot \beta = \beta \cdot \alpha \), we can move all
of the $\alpha$ s to the left and all of the $\beta$ s to the right, giving $\alpha^k \cdot \beta^k$.

(ii) Let $\alpha = (12)$ and $\beta = (13)$.

**Page 114, 2.26:**

(i) Show that $\alpha$ moves $i$ iff $\alpha^{-1}$ moves $i$, for all $\alpha \in S_n$.

(ii) Show that if $\alpha, \beta \in S_n$ are disjoint and $\alpha \beta = 1$, then $\alpha = \beta = 1$.

**Proof.** (i) If $\alpha(i) = j, j \neq i$ and $\alpha^{-1}(i) = i$, then $\alpha \alpha^{-1}(i) = \alpha(i) = j$, a contradiction since $\alpha \alpha^{-1} = 1$. The converse is similar.

(ii) If $\beta(i) = j, j \neq i$, then $\alpha(j) = j$ since they are disjoint, and so $\alpha \beta(i) = j$, contradicting: $\alpha \beta = 1$. Thus $\beta(i) = i$ for all $i$ and $\beta = 1$. Therefore $\alpha = 1$.

**Page 115, 2.29:**

Find nontrivial permutations $\alpha, \beta, \gamma$ in $S_5$ such that $\alpha \beta = \beta \alpha$, $\alpha \gamma = \gamma \alpha$, but $\beta \gamma \neq \gamma \beta$.

**Proof.** Let $\alpha = (12), \beta = (34), \gamma = (35)$.

**Page 115, 2.30:**

Show that if $\alpha \in S_n$ commutes with every $\beta \in S_n$, $n \geq 3$, then $\alpha = 1$.

**Proof.** Suppose that $\alpha$ commutes with all permutations in $S_n$ and $\alpha \neq 1$. Then there are distinct integers, $i, j$ such that $\alpha(i) = j$. Let $k$ be a third integer, different from $i$ and $j$ and let $\beta = (jk)$. Thus $\alpha \beta(i) = \alpha(i) = j$, while $\beta \alpha(i) = \beta(j) = k$. Thus $\alpha \beta \neq \beta \alpha$ and therefore $\alpha = 1$.

**Page 133, 2.37:**

If $y$ is a group element of order $m = pt$ for some prime $p$, show that $y^t$ has order $p$.

**Proof.** Clearly $(y^t)^p = y^{pt} = e$. By Lemma 2.24, the order of $y^t$ must divide $p$. But $p$ is a prime and so the order of $y^t$ is either 1 or $p$. But $y^t \neq e$ and so its order must be $p$.

**Page 133, 2.39:** Let $G = GL(2, Q)$ and let $A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ and $B = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}$. Show that $A^4 = E = B^6$, but that $(AB)^n \neq E$ for all $n > 0$.

**Proof.** We can show that $A^4 = E = B^6$ by direct calculation.

Now consider $AB = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$.

$(AB)^2 = \begin{pmatrix} 1 & -2 \\ 0 & 1 \end{pmatrix}$ and we can show by induction that $(AB)^n = \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix}$. Thus $(AB)^n \neq E$ for all $n > 0$.童
Page 134, 2.41:
Let $G$ be a group in which $x^2 = e$ for all elements $x \in G$. Show that $G$ is abelian.

Proof. Let $a, b \in G$. Then $(ab)^2 = abab = e$. Now consider the equation $abab = e$, multiply on the right by $b^{-1}$ and on the left by $a^{-1}$ giving $ba = a^{-1}b^{-1}$. But since every element satisfies $x^2 = e$, each element is its own inverse. Therefore $ba = a^{-1}b^{-1} = ab$ and so $G$ is abelian.

Page 134, 2.42:
Suppose that $G$ is a group with an even number of elements. Show that the number of elements of order 2 is odd.

Proof. Let $A$ be the elements of $G$ of odd order, not including the identity. Each element of $A$ can be paired with its inverse which is also an element of $A$. Thus $A$ has an even number of elements. If there are an even number of elements of order 2 in $G$, then together with the identity and $A$, there would be an odd number of elements in $G$, contradiction. Thus there are an odd number of elements in $G$ of order 2.

Page 142, 2.51: Show that if $G$ is a cyclic group of order $n$ and $d|n$, then $G$ has a subgroup of order $d$.

Proof. Since $d|n$, then $n = dk$, for some $k$. Let $a$ be a generator of $G$ and consider $a^k$. Clearly $(a^k)^d = a^{kd} = e$. If the order of $a^k$ were smaller than $d$, then the order of $a$ would be smaller than $n$, contradiction. Therefore $a^k$ has order $d$ and so generates a subgroup of order $d$.

Page 142, 2.50:
Prove that every subgroup of a cyclic group is cyclic.

Proof. Let $G = \langle a \rangle$ and Let $H \leq G$. Thus $H = \{a^{s_1}, a^{s_2}, \ldots, a^{s_i}, \ldots\}$. Now among the powers $s_i$, there must be at least one positive integer. For if $a^{s_i} \in H$, then $a^{-s_i} \in H$, since $H$ is a subgroup of $G$. Thus let $s$ be the smallest positive integer among the $s_i$ and we will show that $a^s$ generates $H$. If $a^{s_j} \in H$, then dividing $s_j$ by $s$, we get

$$s_j = s \cdot q + r,$$

$$0 \leq r < s.$$

Thus $a^{s_j} = a^{s \cdot q + r} = a^{s \cdot q} \cdot a^r = (a^s)^q \cdot a^r$. Now since $a^{s_j}, (a^s)^q \in H$, then $a^r \in H$. But $s$ was the smallest positive integer such that $a^s \in H$. Therefore $r = 0$ and $a^{s_j} = (a^s)^q$, whence $H = \langle a^s \rangle$.

Page 177, 2.85: Let the finite group $G$ have a normal subgroup $K$ with $([G : K], |K|) = 1$. Prove that $K$ is the unique subgroup of $G$ of order $|K|$.

Proof. First recall that $[G : K] = |G/K|$. Suppose that $G$ has another subgroup $H$ with $|H| = |K|$. Since $K$ is normal in $G$, $HK$ is a subgroup of $G$ and $K$ is normal in $HK$. The Second Isomorphism Theorem states that

$$HK/K \cong H/H \cap K.$$
Now, on the one hand, $HK/K$ is a subgroup of $G/K$ and so $|HK/K| = r$ divides $|G/K| = [G : K]$. On the other hand, $H/H \cap K$ is a quotient group of $H$ and so $|H/H \cap K| = r$ divides $|H| = |K|$. Thus $r$ divides both $[G : K]$ and $|K|$ which are relatively prime. Therefore $r = |HK/K| = 1$ and so $HK = K$ which implies that $H \leq K$. But $|H| = |K|$ and so $H = K$. 