1. (i) Let $H$ be a normal subgroup of the group $G$. Show that if the index of $H$ in $G$ is $n$, then $g^n \in H$ for every $g \in G$.
(ii) Show by example that if $H$ is not a normal subgroup of $G$, then the conclusion may not be true.

**SOLUTION**: (i) Since the index of $H$ in $G$ is $n$, $|G/H| = n$. Then by Lagrange’s Theorem, $(gH)^n = H$, for all $gH \in G/H$. But $(gH)^n = g^nH$ and so $g^nH = H$ and therefore $g^n \in H$.
(ii) Let $H = \{1, (12)\}$ in $S_3$. Then the index of $H$ in $G$ is 3. Now let $g = (13)$, and $(13)^3 = (13)$, but $(13) \notin H$.

2. Let $G$ be a group of order $p^2$, where $p$ is a prime.
   i) Show that $G$ has at least one subgroup of order $p$.
   ii) (Extra Credit) Show that $G$ has at most $p + 1$ subgroups of order $p$.

**SOLUTION**: (i) Let $g \in G$, $g \neq e$. Then $|g| = p$ or $p^2$. If $|g| = p$, then we are done. If $|g| = p^2$, then $|g^p| = p$.
(ii) Since $p$ is a prime, the only proper subgroup of a group of order $p$ is $\{e\}$. Thus two different subgroups of order $p$ intersect in the identity only. Hence if there are $n$ subgroups of order $p$, each contains $p - 1$ elements of order $p$ not shared with any other subgroup of order $p$. Thus there are exactly $n(p - 1) + 1$ elements of $G$ in those $n$ subgroups of order $p$. Therefore $n(p - 1) + 1 \leq p^2$, whence $n(p - 1) \leq p^2 - 1 = (p - 1)(p + 1)$ and so $n \leq p + 1$.

3. Suppose that $G = A \times B$, the direct product of $A$ and $B$. Show that if $A$ is a cyclic group of order 3 and $B$ is a cyclic group of order 4, then $G$ is a cyclic group of order 12.

**SOLUTION**: If $(a, b) \in A \times B$, then $(a, b)^r = (a^r, b^r)$. Hence if $(a^r, b^r) = (e, e)$, then $r$ is divisible by the orders of $a$ and $b$ and so the order of $(a, b)$ is the lcm($|a|, |b|$).
If $A = \langle x \rangle$ and $B = \langle y \rangle$ with $|x| = 3$ and $|y| = 4$, then $|(x, y)| = 12$. But $|A \times B| = 12$ and therefore $A \times B$ is cyclic of order 12.

4. Let $S_3$ be the symmetric group on 3 letters and let $C_3$ be the cyclic group of order 3. Show that there is no homomorphism from $S_3$ to $C_3$ which is surjective.
**SOLUTION:** Suppose there were such a homomorphism $f$. Then since the image of $f$ is $C_3$, by the First Isomorphism Theorem,

$$S_3/\ker(f) \simeq C_3.$$  

It follows that $|\ker(f)| = 2$. But $S_3$ has no normal subgroups of order 2 since each subgroup of order 2 is of the form $\{1, (ab)\}$ and $(ac)(ab)(ac)^{-1} = (cb) \not\in \{1, (ab)\}$ for $\{a, b, c\} = \{1, 2, 3\}$.

5. An element $[a] \in \mathbb{Z}_n$ is called a *unit* if there is an element $[b] \in \mathbb{Z}_n$ such that $[a] \cdot [b] = [1]$. The set of all units of $\mathbb{Z}_n$ form a multiplicative group $U(\mathbb{Z}_n)$, with $[r] \cdot [s] = [rs]$. Find all elements of $\mathbb{Z}_{14}$ which are units. Describe the group $U(\mathbb{Z}_{14})$.

**SOLUTION:** $[a]$ is a unit in $\mathbb{Z}_{14}$ if and only if $(a, 14) = 1$. Therefore the units of $\mathbb{Z}_{14}$ are $\{[1], [3], [5], [9], [11], [13]\}$. Now consider the powers of $[3] : [3]^2 = [9], [3]^3 = [13]$. Thus $[3]$ is an element of $U(\mathbb{Z}_{14})$ whose order is greater than 3. But $|U(\mathbb{Z}_{14})| = 6$ and so $|[3]| = 6$. Thus $U(\mathbb{Z}_{14})$ has an element of order 6 and so is cyclic of order 6.