1. $H$ and $K$ are subgroups of $G$, $x, y \in G$. Prove if $xH \cap yK \neq \emptyset$, then $xH \cap yK = g(H \cap K)$ for some $g \in G$.

**Solution:** Let $g \in xH \cap yK$, then $g \in xH$ implies $gH = xH$, and $g \in yK$ implies $gK = yK$.

$xH \cap yK = gH \cap gK = g(H \cap K)$.

2. If $G$ is a group of order $p^n$, where $p$ is a prime and $n > 1$. Prove $G$ contains an element of order $p$.

**Solution:** Pick any non-identity element $x \in G$. $|x|$ divides $|G| = p^n$, so $|x| = p^r$ for some $1 \leq r \leq n$.

If $r = 1$, then $x$ is an element of order $p$, done.

If $r > 1$, consider the element $y = x^{p^{r-1}}$: $y^p = (x^{p^{r-1}})^p = x^{p^r} = 1$, so $|y| = p$ if we can show $y \neq 1$.

Suppose $y = 1$, then this is to say $x^{p^{r-1}} = 1$, contradict to $|x| = p^r$, we conclude that $y \neq 1$.

3. If $G$ has five subgroups of order 7, prove $G$ has at least 35 elements.

**Solution:** If $H$ and $K$ are two subgroups of order 7 in $G$ such that $H \neq K$, then $H \cap K = \{1\}$: Suppose there is non-identity $x \in H \cap K$, then in particular, $x \in H$, so $|x|$ divides $|H| = 7$, and $x$ is not the identity, it follows $|x| = 7$, so $< x > = H$. Similarly, $< x > = K$, we get $H = K$, contradict to the assumption $H \neq K$, therefore such $x$ does not exists. we conclude $H \cap K = \{1\}$.

If there are five different subgroups of order 7, then by the above paragraph, except the identity element, any two of those five subgroups share no element. It follows there are $1 + 5 \times (7 - 1) = 31$ elements in the union of these five subsets, so $|G| \geq 31$.

$G$ contains subgroups of order 7 implies 7 divides $|G|$, and 35 is the smallest multiple of 7 that is no smaller than 31, so we conclude $|G| \geq 35$. 


4. \( G \) is a group of order 25. If \( G \) has only one subgroup of order 5, prove \( G \) is cyclic.

**Solution:** If the only cyclic subgroup of order 5 is \(< x >\), let \( y \in G \) and \( y \notin < x >\). \(|y| \) divides \(|G| = 25\), \( y \neq 1 \) since it is not the identity, \(|y| \neq 5\) otherwise there will be another cyclic subgroup of order 5, so \(|y| = 25\), \( G = < y >\) is cyclic.

5. Prove that every subgroup of index two is a normal subgroup.

**Solution:** When \( g \in H \), it is obvious that \( gHg^{-1} = H \).

When \( g \notin H \), since the index of \( H \) is two, there are two left cosets \( H \) and \( gH \), two right cosets \( H \) and \( Hg \). Since cosets make a partition of \( G \),

\[
H \sqcup gH = G = H \sqcup Hg
\]

This implies \( gH = Hg \), i.e. \( gHg^{-1} = H \).

We conclude \( gHg^{-1} = H \) for all \( g \in G \), so \( H \) is a normal subgroup of \( G \).

6. \( \overline{a} \in \mathbb{Z}/n\mathbb{Z} \) and \( \overline{a} \neq \overline{0} \), what is the order of \( \overline{a} \) in \( \mathbb{Z}/n\mathbb{Z} \)?

**Solution:** \( ka = \overline{0} \iff \overline{ka} = \overline{0} \iff ka \in n\mathbb{Z} \iff ka \in n\mathbb{Z} \cap a\mathbb{Z} \iff ka \in m\mathbb{Z} \) where \( m \) is the least common multiple of \( a \) and \( n \). So we see

\[
k \in \frac{m}{a}\mathbb{Z}
\]

\( |\overline{a}| \), the smallest positive choice for \( k \), is \( k = \frac{m}{a} = \frac{n}{g} \), where \( g \) is the greatest common divisor of \( a \) and \( n \).

7. Is \( Aut(\mathbb{Z}/8\mathbb{Z}) \) isomorphic to \( Aut(\mathbb{Z}/10\mathbb{Z}) \)? Why?

**Solution:** \( Aut(\mathbb{Z}/8\mathbb{Z}) \cong (\mathbb{Z}/8\mathbb{Z})^\times = \{1, 3, 5, 7\} \).

\( Aut(\mathbb{Z}/10\mathbb{Z}) \cong (\mathbb{Z}/10\mathbb{Z})^\times = \{1, 3, 7, 9\} \).

So The order of both groups are 4.

They are not isomorphic since in \( (\mathbb{Z}/8\mathbb{Z})^\times \), all the non-identity elements have order 2 but in \( (\mathbb{Z}/10\mathbb{Z})^\times \), there are elements (3 and 7) of order 4.

8. \( m \geq 2, n \geq 2 \) are positive integers and they are relatively prime. \( a, b \in \mathbb{Z} \).

Prove there exists \( k, l \in \mathbb{Z} \) such that \( x = anl + bmk \) is a solution to the system of equations

\[
\begin{align*}
x &\equiv a \pmod{m} \\
x &\equiv b \pmod{n}
\end{align*}
\]
Solution: $m$ and $n$ are relatively prime, so $\bar{m} \in (\mathbb{Z}/n\mathbb{Z})^\times$ and $\bar{n} \in (\mathbb{Z}/m\mathbb{Z})^\times$, there exists $\bar{k} \in (\mathbb{Z}/n\mathbb{Z})^\times$ such that $\bar{m}\bar{k} = \bar{1} \in \mathbb{Z}/n\mathbb{Z}$, and there exists $\bar{l} \in (\mathbb{Z}/m\mathbb{Z})^\times$ such that $\bar{n}\bar{l} = \bar{1} \in \mathbb{Z}/m\mathbb{Z}$.

In $\mathbb{Z}/m\mathbb{Z}$: $\bar{x} = \bar{a}n\bar{l} + \bar{b}mk = \bar{a}n\bar{l} = \bar{a}\bar{1} = \bar{a}$, so $x \equiv a \pmod{m}$.

In $\mathbb{Z}/n\mathbb{Z}$: $\bar{x} = \bar{a}n\bar{l} + \bar{b}mk = \bar{b}mk = \bar{b}\bar{1} = \bar{b}$, so $x \equiv b \pmod{n}$.

Remark 0.1. $k$ and $l$ can be chosen to be the numbers making $mk + nl = 1$, such $k, l$ exist since $m, n$ are relatively prime. In practice, to find explicit values of $k$ and $l$, you need to apply the Euclidean Algorithm (https://en.wikipedia.org/wiki/Euclidean_algorithm) to the pair $(m, n)$. 