WEEK 8  SAMPLE SOLUTIONS

These solutions are just samples. There are other approaches to the problems that are also correct.

1. Given are \( n_1, \ldots, n_\ell \). As in the assignment, let

\[ H = \{ n_1 \cdot p_1 + n_2 \cdot p_2 + \cdots + n_\ell \cdot p_\ell \mid p_1, p_2, \ldots, p_\ell \in \mathbb{Z} \}. \]

We first show that \((H, +)\) is a subgroup of \((\mathbb{Z}, +)\). Here we use Proposition 2.3. Applied to the group \((\mathbb{Z}, +)\), this proposition says that \((H, +)\) is a subgroup of \((\mathbb{Z}, +)\) if and only if \( a + (-b) \in H \) whenever \( a, b \in H \). So let \( a, b \in H \) be arbitrary. Say

\[
\begin{align*}
    a &= n_1 \cdot p_1 + n_2 \cdot p_2 + \cdots + n_\ell \cdot p_\ell \quad \text{for some } p_1, p_2, \ldots, p_\ell \in \mathbb{Z} \\
    b &= n_1 \cdot p'_1 + n_2 \cdot p'_2 + \cdots + n_\ell \cdot p'_\ell \quad \text{for some } p'_1, p'_2, \ldots, p'_\ell \in \mathbb{Z}.
\end{align*}
\]

An easy computation then yields:

\[ a + (-b) = n_1 \cdot (p_1 - p'_1) + n_2 \cdot (p_2 - p'_2) + \cdots + n_\ell \cdot (p_\ell - p'_\ell). \]

Since \( p_i - p'_i \in \mathbb{Z} \) for all \( i \in \{1, 2, \cdots, \ell\} \), we see that \( a + (-b) \in H \). So we conclude that \((H, +)\) is a subgroup of \((\mathbb{Z}, +)\).

Now we apply Proposition 3.3. Since \((\mathbb{Z}, +)\) is a cyclic group, every subgroup of \((\mathbb{Z}, +)\) is cyclic as well. In particular, \((H, +)\) is cyclic.

Let \( d \) be the positive generator of the group \((H, +)\). Since \( d \) is a generator of \((H, +)\), every element of \( H \) is of the form \( m \cdot d \) for some \( m \in \mathbb{Z} \). It follows that every element of \( H \) is divisible by \( d \).

Now show that \( d \) is the greatest common divisor of \( n_1, n_2, \ldots, n_\ell \).

\[(a) \quad d \mid n_i \text{ for all } i \in \{1, 2, \cdots, \ell\}. \] To see this, it suffices to show that \( n_i \in H \) for all \( i \in \{1, 2, \cdots, \ell\} \), since we have just seen that all elements of \( H \) are divisible by \( d \). But

\[ n_i = 0 \cdot n_1 + \cdots + 0 \cdot n_{i-1} + 1 \cdot n_i + 0 \cdot n_{i+1} + \cdots + 0 \cdot n_\ell, \]

so indeed \( n_i \in H \).
(b) Assume $d' | n_i$ for all $i \in \{1, 2, \ldots, \ell\}$. We show that $d' | d$. Since $d' | n_i$, there is some $q_i \in \mathbb{Z}$ such that $n_i = d' \cdot q_i$. Now $d$ is a generator of $(H, +)$, so in particular $d \in H$, so there are some $p_1, \ldots, p_\ell$ such that

$$d = n_1 \cdot p_1 + n_2 \cdot p_2 + \cdots + n_\ell \cdot p_\ell.$$ 

Now substitute $n_i = d' \cdot q_i$ into this equation. We obtain

$$d = d' \cdot q_1 \cdot p_1 + d' \cdot q_2 \cdot p_2 + \cdots + d' \cdot q_\ell \cdot p_\ell = d' \cdot (q_1 \cdot p_1 + q_2 \cdot p_2 + \cdots + q_\ell \cdot p_\ell).$$

Since the sum in the parentheses on the right side gives an integer number, we see that $d' | d$.

2. Given are integers $n_1, \ldots, n_\ell$. We proceed similarly as in Problem 1. First, show that

$$H = \text{the set of all common multiples of } n_1, \ldots, n_\ell$$

is a subgroup of $(\mathbb{Z}, +)$. So let $a, b \in H$. We have to show that $a + (-b) \in H$. This amounts to showing that $a + (-b)$ is a common multiple of $n_1, \ldots, n_\ell$. Equivalently, that $n_i | a + (-b)$ for all $i \in \{1, 2, \ldots, \ell\}$. Fix such an $i$. Since $a \in H$, $a$ is a multiple of $n_i$, so $a = n_i \cdot p$ for some $p \in \mathbb{Z}$. Similarly, since $b \in H$, $b = n_i \cdot p'$ for some $p' \in \mathbb{Z}$. Then

$$a + (-b) = n_i \cdot p - n_i \cdot p' = n_i \cdot (p - p').$$

Since $p - p' \in \mathbb{Z}$, we see that $a + (-b)$ is a multiple of $n_i$, and this is true for all $i \in \{1, 2, \ldots, \ell\}$. So $a + (-b) \in H$. Conclusion: $(H, +)$ is a subgroup of $(\mathbb{Z}, +)$. As before we use Proposition 3.3 to conclude that $(H, +)$ is cyclic. Let $m$ be the positive generator of $(H, +)$.

Now show that $m$ is the smallest common multiple of $n_1, \ldots, n_\ell$.

(a) Show that $m$ is a multiple of $n_1, \ldots, n_\ell$. But $n$ is a generator of $(H, +)$, so in particular $n \in H$. Hence $n$ is a common multiple of $n_1, \ldots, n_\ell$, since all elements of $H$ are such multiples.

(b) Assume $m'$ is a common multiple of $n_1, \ldots, n_\ell$. Show that $m | m'$. Since $m'$ is a common multiple of $n_1, \ldots, n_\ell$, we have $m' \in H$. Since $m$ is a generator of $(H, +)$, there is some $p \in \mathbb{Z}$ such that $m' = m \cdot p$. But this tells us that $m | m'$. 

2
3. Here we use Proposition 3.6. Clause (b) of this proposition tells us that 
\[< n >\] has \(p \cdot q / \text{gcd}(p \cdot q, n)\) elements. So \(< n > = \mathbb{Z}_{p \cdot q}\) if and only the value of 
this fraction is equal to \(p \cdot q\), which happens precisely when \(\text{gcd}(p \cdot q, n) = 1\). 
So it suffices to find all numbers \(n \in \mathbb{Z}_{p \cdot q}\) such that \(\text{gcd}(p \cdot q, n) = 1\).

Now, by the hint, the product \(p \cdot q\) has only three divisors that are in \(\mathbb{Z}_{p \cdot q}\), 
namely \(p, q\) and \(1\). Thus, if \(n \in \mathbb{Z}_{p \cdot q}\), then \(\text{gcd}(n, p \cdot q) = 1\) if and only if \(n\) is 
not divisible by \(p\) or \(q\).

Now all numbers in \(\mathbb{Z}_{p \cdot q}\) that are divisible by \(p\) are
\[
0, p, p \cdot 2, \ldots, p \cdot (q - 1),
\]
and all these numbers are mutually distinct. Now all numbers in \(\mathbb{Z}_{p \cdot q}\) that 
are divisible by \(q\) are
\[
0, q, q \cdot 2, \ldots, q \cdot (p - 1),
\]
and all these numbers are mutually distinct. We show that
\[
p, p \cdot 2, \ldots, p \cdot (q - 1), q, q \cdot 2, \ldots, q \cdot (p - 1)
\]
are mutually distinct. To see this, it is enough to show that \(p \cdot m \neq q \cdot m'\) 
whenever \(m \in \{1, 2, \ldots, q - 1\}\) and \(m' \in \{1, 2, \ldots, p - 1\}\). But if for some 
such \(m, m'\) we would have
\[
p \cdot m = q \cdot m'.
\]
Since \(p\) is a prime, either \(p \mid q\) or \(p \mid m'\). But the former is impossible since we 
are assuming that \(p, q\) are distinct primes, and the latter is impossible since 
\(1 \leq m' < p\). So \(p \cdot m \neq q \cdot m'\) after all.

Conclusion: \(< n > \neq \mathbb{Z}_{p \cdot q}\) if and only if \(n\) is one of the numbers
\[
0, p, p \cdot 2, \ldots, p \cdot (q - 1), q, q \cdot 2, \ldots, q \cdot (p - 1).
\]
There are \(1 + (q - 1) + (p - 1) = p + q - 1\) such numbers. Thus, \(< n > = \mathbb{Z}_{p \cdot q}\) if 
and only if \(n\) is not among the above numbers, so there are \(p \cdot q - (p + q - 1) =
\]
\(p \cdot (q - 1) - (q - 1) = (p - 1) \cdot (q - 1)\) such numbers \(n\).