**Problem 1.** Let $I = n\mathbb{Z}$ and $J = m\mathbb{Z}$ be ideals of $\mathbb{Z}$.

a) Prove that $I + J = \text{gcd}(m, n)\mathbb{Z}$.

b) Prove that $I \cap J = [m, n]\mathbb{Z}$, where $[m, n]$ is the least common multiple of $m$ and $n$.

c) Prove that $IJ = (mn)\mathbb{Z}$.

d) Prove that $I \subseteq J$ iff $m|n$.

**Solution:**

a) Since $\text{gcd}(m, n)|n$, any multiple of $n$ is also a multiple of $\text{gcd}(m, n)$. Thus $I \subseteq \text{gcd}(m, n)\mathbb{Z}$. Similarly, $J \subseteq \text{gcd}(m, n)\mathbb{Z}$. It follows that $I + J \subseteq \text{gcd}(m, n)\mathbb{Z}$ (since $\text{gcd}(m, n)\mathbb{Z}$ is closed under addition).

To get the opposite inclusion recall that $\text{gcd}(m, n) = an + bm$ for some integers $a, b$. Since $an \in I$ and $bm \in J$, we see that $\text{gcd}(m, n) \in I + J$ and therefore $\text{gcd}(m, n)\mathbb{Z} \subseteq I + J$ (since $I + J$ is closed under multiplication by any integer).

We proved that $I + J \subseteq \text{gcd}(m, n)\mathbb{Z}$ and $\text{gcd}(m, n)\mathbb{Z} \subseteq I + J$. It follows that $I + J = \text{gcd}(m, n)\mathbb{Z}$

b) Since $n|[m, n]$, we have $[m, n] \in I$ and consequently $[m, n]\mathbb{Z} \subseteq I$. Similarly, $[m, n]\mathbb{Z} \subseteq J$. It follows that $[m, n]\mathbb{Z} \subseteq I \cap J$.

On the other hand, if $k \in I \cap J$ then $n|k$ and $m|k$ and therefore $[m, n]|k$ so $k \in [m, n]\mathbb{Z}$. This proves that $I \cap J \subseteq [m, n]\mathbb{Z}$.

We proved that $[m, n]\mathbb{Z} \subseteq I \cap J$ and $I \cap J \subseteq [m, n]\mathbb{Z}$ so we have $I \cap J = [m, n]\mathbb{Z}$.

c) A product of a multiple of $n$ and a multiple of $m$ is a multiple of $mn$ and the sum of any number of multiples of $mn$ is a multiple of $mn$. Since every element in $IJ$ is a sum of some number of products of an element from $I$ by an element from $J$, we see that each element in $IJ$ is a multiple of $mn$. Conversely, any multiple of $mn$ is a product of $n \in I$ and a multiple of $m$ which is in $J$, hence it is in $IJ$. This proves that $IJ = (mn)\mathbb{Z}$.

**Remark** It is easy to see that in any commutative ring $R$ we have $(rR)(sR) = (rs)R$.

d) Suppose that $m|n$. Then $n \in m\mathbb{Z}$ and therefore $I = n\mathbb{Z} \subseteq m\mathbb{Z} = J$. Conversely, if $I \subseteq J$ then $n \in J$ (since $n \in I$), so $m|n$. 


Problem 2. Let $R$ be a ring. Two ideals $I$, $J$ of $R$ are called **coprime** if $I + J = R$. Suppose that $I$ and $J$ are coprime.

a) Prove that for any $r, t \in R$ there is $s \in R$ such that $s + I = r + I$ and $s + J = t + J$. **Hint:** Write $r = i + j$, $t = i_1 + j_1$ for some $i, i_1 \in I$ and $j, j_1 \in J$ and consider $s = j + i_1$.

b) Let $f_1 : R \to R/I$ and $f_J : R \to R/J$ be the cannonical homomorphisms. Define $f : R \to (R/I) \oplus (R/J)$ by $f(r) = (f_1(r), f_J(r))$. Use a) to prove that $f$ is a surjective ring homomorphism. What is $\ker f$?

c) Prove that $R/(I \cap J)$ is isomorphic to $(R/I) \oplus (R/J)$. Conclude that $\mathbb{Z}/(mn)\mathbb{Z}$ is isomorphic to $\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$ for any relatively prime positive integers $m, n$ (compare this to the Chinese remainder theorem and the map $r$ of Lemma 1.6.3 in Lauritzen’s book.

d) Let $R$ be unital and commutative. Prove that $I \cap J = IJ$. **(Hint:** Write $1 = i + j$ for some $i \in I$, $j \in J$ and use the fact that $x = 1 \cdot x$ for any $x$.) Conclude that $[m, n] = mn$ for relatively prime positive integers $m, n$.

**Solution:** a) Since $R = I + J$ any element of $R$ can be written as $i + j$ for some $i \in I$ and $j \in J$. In particular, $r = i + j$, $t = i_1 + j_1$ for some $i, i_1 \in I$ and $j, j_1 \in J$. Let $s = j + i_1$. Since $s - r = i_1 - i \in I$, we have $s + I = r + I$. Similarly, since $s - t = j - j_1 \in J$, we have $s + J = t + J$.

b) Note first the following general fact. If $R, S, T$ are rings and $g : R \to S$, $h : R \to T$ are homomorphisms then the map $f : R \to S \oplus T$ given by $f(r) = (g(r), h(r))$ is a ring homomorphism. In fact,

\[ f(r + t) = (g(r + t), h(r + t)) = (g(r) + g(t), h(r) + h(t)) = (g(r), h(r)) + (g(t), h(t)) = f(r) + f(t), \]

and

\[ f(r \cdot t) = (g(r \cdot t), h(r \cdot t)) = (g(r) \cdot g(t), h(r) \cdot h(t)) = (g(r), h(r)) \cdot (g(t), h(t)) = f(r) \cdot f(t). \]

Furthermore, $f(r) = 0 = (0, 0)$ iff $g(r) = 0$ and $h(r) = 0$. This means that $\ker f = \ker g \cap \ker h$.

This proves that the $f$ defined in the problem is a homomorphism and $\ker f = I \cap J$. It remains to prove that $f$ is surjective (this is the main meassage of the
problem). By a), given \((r + I, t + J) \in (R/I) \oplus (R/J)\) there is \(s \in R\) such that 
\[(r + I, t + J) = (s + I, s + J) = (f_I(s), f_J(s)) = f(s)\]. This proves that \(f\) is surjective.

c) According to b), the map \(f\) is a surjective homomorphism from \(R\) to \((R/I) \oplus (R/J)\) and \(\ker f = I \cap J\). By the First Homomorphism Theorem, the rings \(R/(I \cap J)\) and \((R/I) \oplus (R/J)\) are isomorphic. The actual isomorphism \(g\) is given by \(g(r + (I \cap J)) = (r + I, r + J)\).

Let us apply this to the case when \(R = \mathbb{Z}, I = n\mathbb{Z}, J = m\mathbb{Z}\) for some relatively prime integers \(m, n\). By a) of the previous problem, we have \(I + J = \gcd(m, n)\mathbb{Z} = \mathbb{Z} = R\), so \(I, J\) are coprime. Since \(\gcd(m, n) = 1\), we have \([m, n] = mn\). It follows from b) of the previous problem that \(I \cap J = mn\mathbb{Z}\). Thus \(\mathbb{Z}/(mn)\mathbb{Z}\) is isomorphic to \(\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}\). (Note that the map \(g\) in this case coincides with the \(r\) of Lemma 1.6.3 in Lauritzen’s book, so we can consider this result as a special case of Chinese remainder theorem.)

d) It is always true that \(IJ \subseteq I \cap J\). Thus it suffices to show that if \(I, J\) are coprime and \(R\) is commutative and unital then \(I \cap J \subseteq IJ\). Let \(r \in I \cap J\). Since \(R = I + J\), we have \(1 = i + j\) for some \(i \in I\) and \(j \in J\). Thus

\[r = r \cdot 1 = r(i + j) = ri + rj = ir + rj \in IJ.\]

In the special case, when \(R = \mathbb{Z}, I = n\mathbb{Z}, J = m\mathbb{Z}\) for some relatively prime integers \(m, n\) (we have already seen that \(I, J\) are coprime) we get by b) and c) of the previous problem that \([m, n]\mathbb{Z} = I \cap J = IJ = mn\mathbb{Z}\). Since \(mn\) and \([m, n]\) are positive, we get that \(mn = [m, n]\).