Problem 1. Let R be an integral domain and let $a, b \in R$. An element $m \in R$ is called a **least common multiple** of a and b if

1. $a|m$ and $b|m$
2. if $c \in R$ and $a|c$ and $b|c$ then $m|c$.

a) Prove that if m_1 and m_2 are least common multiples of a and b then m_1 and m_2 are associated (so, a least common multiple, if exists, is unique up to an invertible factor).

b) Let R be a UFD. We proved that $\gcd(a, b)$ exists for any $a, b \in R$. Let a, b be nonzero elements of R. Prove that $a/\gcd(a, b)$ and $b/\gcd(a, b)$ are relatively prime.

c) Suppose that R is a UFD. Let a, b be nonzero elements of R. Prove that $ab/\gcd(a, b)$ is a least common multiple of a and b. Thus least common multiples exist in any UFD.

Solution: a) Since m_1 is a least common multiple of a and b and both a, b divide m_2, we have $m_1|m_2$. Switching the roles of m_1 and m_2 in the last argument, we get $m_2|m_1$. Thus m_1 and m_2 are associated.

b) Suppose that x is a divisor of $a/\gcd(a, b)$ and $b/\gcd(a, b)$. Then $x\gcd(a, b)$ divides both a and b, so $x\gcd(a, b)|\gcd(a, b)$. Canceling by $\gcd(a, b)$, we get that $x|1$, i.e. x is invertible. We showed that any common divisor of $a/\gcd(a, b)$ and $b/\gcd(a, b)$ is invertible. This means that $a/\gcd(a, b)$ and $b/\gcd(a, b)$ are relatively prime.

Remark. Note that we only used the existence of $\gcd(a, b)$ in the above argument. In other words we proved that if $\gcd(a, b)$ exists for two non-zero elements a, b in an integral domain (we do not assume that it is UFD), then $a/\gcd(a, b)$ and $b/\gcd(a, b)$ are relatively prime.

c) Clearly $ab/\gcd(a, b) = a(b/\gcd(a, b)) = (a/\gcd(a, b))b$ is divisible both by a and by b. Suppose that $a|m$ and $b|m$ for some $m \in R$. It follows that $\gcd(a, b)|m$ and

$$\frac{a}{\gcd(a,b)} \Big| \frac{m}{\gcd(a,b)}, \quad \frac{b}{\gcd(a,b)} \Big| \frac{m}{\gcd(a,b)}.$$

We proved that in a UFD if two relatively prime elements x, y divide a third element z then also $xy|z$. Since $a/\gcd(a, b)$ and $b/\gcd(a, b)$ are relatively prime by b), we conclude that

$$\frac{a}{\gcd(a,b)}\frac{b}{\gcd(a,b)}|\frac{m}{\gcd(a,b)}.$$

Multiplying by $\gcd(a,b)$ we see that $ab/\gcd(a,b)$ divides m. This proves that $ab/\gcd(a,b)$ is a least common multiple of a and b.

Problem 2. Let R be an integral domain.

a) Let $f,g \in R[x]$ be such that $fg = cx^n$ for some n and some $c \in R$, $c \neq 0$. Prove that there exist elements $a,b \in R$ and $m \leq n$ such that $f = ax^m$ and $g = bx^{n-m}$ and $ab = c$.

b) Suppose that $f = f_0 + f_1x + ... + f_nx^n \in R[x]$. Suppose that there is a prime ideal P of R such that $f_n \notin P$, $f_0, ..., f_{n-1} \in P$ and $f_0 \notin P^2$. Prove that if $f = gh$ for some $g,h \in R[x]$ then one of g,h is constant. Conclude that if in addition f is monic then it is irreducible in $R[x]$. This result is known as **Eisenstein criterion**. Hint: Assume that $f = gh$ and both g,h have positive degree. Pass to the ring $(R/P)[x]$ and apply a) to show that constant terms of g and h belong to P. Derive contradiction.

c) Prove that the polynomial $2x^{10} + 21x^8 - 35x^2 + 14$ is irreducible in $\mathbb{Z}[x]$. Hint: Apply Eisenstein criterion with appropriate prime ideal P.

Solution: a) Let $m = \deg f$ and let a,b be the leading coefficients of f, g respectively. Since $fg = cx^n$, comparing leading coefficients and degrees of both sides yields $ab = c$ and $n - m = \deg g$. Suppose that smallest power of x which occurs in f with non-zero coefficient is x^k and the smallset power of x occuring in g with non-zero coefficient is l. Then $k \leq m$, $l \leq n-m$ and $x^k \cdot x^l = x^{k+l}$ occurs in fg with non-zero coefficient. Thus $k + l = n = m + (n-m)$. It follows that $m = k$ and $n - m = l$ are also the largest powers of x occuring in f, g respectively. In other words, $f = ax^m$, $g = bx^{n-m}$.

b) Suppose that $f = gh$ and $\deg g = m > 0$, $\deg h = k > 0$. Thus $k + m = n$. The canonical homomorphism $\phi : R \longrightarrow R/P$ induces a homomorphism $\phi : R[x] \longrightarrow (R/P)[x]$ defined by $\phi(a_0 + a_1x + ... + a_sx^s) = \phi(a_0) + \phi(a_1)x + ... + \phi(a_s)x^s$. Since $f_0, ..., f_{n-1}$ belong to P, they are maped to 0 in R/P, so $\phi(f) = \phi(f_n)x^n$ and $\phi(f_n) \neq 0$ (since $f_n \notin P$). On the other hand, $\phi(f) = \phi(gh) = \phi(g)\phi(h)$. We see that $\phi(f_n)x^n = \phi(g)\phi(h)$ in $(R/P)[x]$. Write $g = g_0 + g_1x + ... + g_mx^m$ and $h = h_0 + h_1x + ... + h_kx^k$. Then $\phi(g) = \phi(g_0) + \phi(g_1)x + ... + \phi(g_m)x^m$ and $\phi(h) = \phi(h_0)+\phi(h_1)x+...+\phi(h_k)x^k$. Comparing degrees in the equality $\phi(f_n)x^n = \phi(g)\phi(h)$ we see that $\phi(g_m) \neq 0$ and $\phi(h_k) \neq 0$. Since P is a prime ideal, the ring R/P is an integral domain so we may apply a) to the ring $(R/P)[x]$. It follows that $\phi(g) = \phi(g_m)x^m$ and $\phi(h) = \phi(h_k)x^k$. Consequently, since both m, k are positive, we must have $\phi(g_0) = 0 = \phi(h_0)$. This means that $g_0 \in P$ and $h_0 \in P$. This however implies that $f_0 = g_0h_0 \in P^2$, a contradiction. This proves that either g or h must be a constant. If in addition f is monic, then this constant is invertible (compare the leading coefficients) so we see that whenever $f = gh$ one of g, h is invertible. This proves that f is irreducible in $R[x]$.

For those still alergic to factor rings here is another, more direct argument. Let s be smallest such that $g_s \notin P$ and let t be smallest such that $h_t \notin P$. Since $f = gh$ we have in particular

$$f_{s+t} = g_sg_t + \sum_{i<s} g_ih_{s+t-i} + \sum_{j<t} g_{s+t-j}h_j.$$

Note that each summand in $\sum_{i<s} g_ih_{s+t-i}$ belongs to P since P is an ideal and $g_i \in P$ for $i < s$. Likewise each summand of $\sum_{j<t} g_{s+t-j}h_j$ belongs to P. Thus the sum $\sum_{i<s} g_ih_{s+t-i} + \sum_{j<t} g_{s+t-j}h_j$ belongs to P. Since P is a prime ideal and neither g_s nor g_t belong to P also $g_sg_t \notin P$. Thus

$$f_{s+t} = g_sg_t + \sum_{i<s} g_ih_{s+t-i} + \sum_{j<t} g_{s+t-j}h_j \notin P.$$

This is only possible if $s+t = n$. Thus $s = m$ and $t = n-m$. In particular, both g_0 and h_0 belong to P. From now on the argument continues as in the first solution.

c) Let $f(x) = 2x^{10} + 21x^8 - 35x^2 + 14$ and let $P = 7\mathbb{Z}$. This is a prime ideal of $\mathbb{Z}$. Clearly $2 \notin P$, $21, -35, 14$ all belong to P and $14 \notin P^2$. Suppose that $f = gh$ for some $g, h \in \mathbb{Z}[x]$. By Eisenstein criterion, either g or h is constant. Without loss of generality we may assume that $g = a$ is a constant. Then all coefficients of f are divisible by a. The only integers which divide all coefficients of f are 1 and -1, so $a = \pm 1$ is invertible. This proves that f is irreducible in $\mathbb{Z}[x]$.