

Homework 1 Solutions

Problem 1.1.18 Give a detailed proof of the statement in the text that if a and b are integers, then $b \mid a$ if and only if $a\mathbb{Z} \subseteq b\mathbb{Z}$.

Proof. ($\Rightarrow$): If $b \mid a$ then $a = bc$ for some $c \in \mathbb{Z}$. Hence if $x \in a\mathbb{Z}$ then $x = ar$ for some $r \in \mathbb{Z}$ and $x = (bc)r = b(cr) \in b\mathbb{Z}$. This shows that $a\mathbb{Z} \subseteq b\mathbb{Z}$.

($\Leftarrow$): Now suppose $a\mathbb{Z} \subseteq b\mathbb{Z}$. Thus $a \in a\mathbb{Z} \subseteq b\mathbb{Z} \Rightarrow a = bc$ for some $c \in \mathbb{Z}$ and hence $b \mid a$. $\square$

Problem 1.1.19 Let $a, b, c \in \mathbb{Z}$, with $b > 0, c > 0$, and let q be the quotient and r the remainder when a is divided by b

(a) Show that q is the quotient and rc is the remainder when ac is divided by bc .

(b) Show that if q' is the quotient when a is divided by c , then q' is the quotient when a is divided by bc .

Proof. (a): By assumption $a = bq + r$ with $0 \leq r < b$ therefore $ac = bcq + rc$ with $0 \leq rc < bc$. This shows that rc is the remainder and q is the quotient when ac is divided by bc .

(b): By assumption $a = cq' + r'$ with $0 \leq r' < c$. Therefore $a = b(cq' + r') + r = bcq' + br' + r$. I claim that $0 \leq br' + r < bc$ and hence $br' + r$ is the remainder and q' is the quotient when a is divided by bc . Since r' is an integer the condition $0 \leq r' < c$ implies that $0 \leq r' \leq c - 1$ and hence $0 \leq br' \leq bc - b$. Noting that $0 \leq r < b$ we then have $0 \leq br' + r \leq bc - b + r < bc$ which completes the proof. $\square$

Problem 1.1.20 Let a, b, n be integers with $n > 1$. Suppose that $a = nq_1 + r_1$ with $0 \leq r_1 < n$ and $b = nq_2 + r_2$ with $0 \leq r_2 < n$. Prove that $n \mid (a - b)$ if and only if $r_1 = r_2$.

Proof. ($\Rightarrow$): Note that $a - b = n(q_1 - q_2) + r_1 - r_2$, so the assumption $n \mid (a - b)$ implies that $n \mid r_1 - r_2$. Hence $r_1 - r_2 = nk$ for some $k \in \mathbb{Z}$ and thus $r_1 - r_2 = 0$ or $|r_1 - r_2| \geq n$. The latter cannot happen since $|r_1 - r_2| < n$. Thus the former must occur, i.e. $r_1 = r_2$.

($\Leftarrow$): The assumption $r_1 = r_2$ implies that $a - b = n(q_1 - q_2)$, i.e. $n \mid (a - b)$. $\square$

Problem 1.1.22 Let a, b, q, r be integers such that $b \neq 0$ and $a = bq + r$. Prove that $(a, b) = (b, r)$ by showing that (b, r) satisfies the definition of the greatest common divisor of a and b .

Proof. To show that (b, r) satisfies the definition of (a, b) we must show: (i) $(b, r) \mid a$ and $(b, r) \mid b$ and (ii) If $c \in \mathbb{Z}$ such that $c \mid a$ and $c \mid b$ then $c \mid (b, r)$.

(i): By definition of (b, r) we have $(b, r) \mid b$ and $(b, r) \mid r$ hence $(b, r) \mid bq + r = a$. Thus (b, r) satisfies (i).

(ii): If $c \mid a$ and $c \mid b$ then $c \mid a - bq = r$. Hence by the definition of (b, r) we must have $c \mid (b, r)$. $\square$

Problem 1.2.12 Let a, b be positive integers, and let $d = (a, b)$. Since $d \mid a$ and $d \mid b$, there exist integers h, k such that $a = dh$ and $b = dk$. Show that $(h, k) = 1$.

Proof. Recall that $d = ax + by$ for some integers x and y . Thus $d = dhx + dky$ and hence $1 = hx + ky$ which shows that $1 = (h, k)$. $\square$

Problem 1.2.14. Show that $a\mathbb{Z} \cap b\mathbb{Z} = [a, b]\mathbb{Z}$.

Proof. Since $a \mid [a, b]$ and $b \mid [a, b]$ it follows that $[a, b]\mathbb{Z} \subseteq a\mathbb{Z}$ and $[a, b]\mathbb{Z} \subseteq b\mathbb{Z}$ so that $[a, b]\mathbb{Z} \subseteq a\mathbb{Z} \cap b\mathbb{Z}$. Now if $x \in a\mathbb{Z} \cap b\mathbb{Z}$ then x is a multiple of a and b and by definition of $[a, b]$, x must also be a multiple of $[a, b]$, that is $x \in [a, b]\mathbb{Z}$. Hence $a\mathbb{Z} \cap b\mathbb{Z} \subseteq [a, b]\mathbb{Z}$ which completes the proof. $\square$

Problem 1.2.20. Show that an integer $a > 1$ is a square if and only if every exponent in its prime factorization is even.

Proof. ($\Rightarrow$): Let n be a positive integer such that $a = n^2$. Then $n > 1$ and has a prime factorization $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ where $p_1 < p_2 < \cdots < p_k$ and $\alpha_i \geq 1$ for all i . Now observe that $a = n^2 = p_1^{2\alpha_1} \cdots p_k^{2\alpha_k}$ and by uniqueness of prime factorization this must be the prime factorization for a . In particular every exponent in the prime factorization of a is even.

($\Leftarrow$): Suppose $a = p_1^{2\alpha_1} \cdots p_k^{2\alpha_k}$ with $p_1 < \cdots < p_k$ and $\alpha_i \geq 1$. Then if $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, $n^2 = a$ with $n \in \mathbb{Z}$, i.e. a is a square. $\square$

Problem 1.2.22. *Show that if a, b are positive integers such that $(a, b) = 1$ and ab is a square, then a and b are also squares.*

Proof. In the case when $a = 1$ and $b = 1$ the result is trivial. Since $(a, b) = 1$ we may then assume that $a > 1$ and $b > 1$. Let $a = p_1^{\alpha_1} \cdots p_n^{\alpha_n}$ and $b = q_1^{\beta_1} \cdots q_m^{\beta_m}$ be the prime factorizations of a and b . Since $(a, b) = 1$, $p_i \neq q_j$ for any i, j . Then $ab = p_1^{\alpha_1} \cdots p_n^{\alpha_n} q_1^{\beta_1} \cdots q_m^{\beta_m}$ is a prime factorization of ab which must have even exponents since it was assumed to be a square. Hence α_i and β_j are even and therefore a and b are squares. $\square$