

Assignment 9 Solutions

Ernest Musafiri Mastaki
Introduction to Mathematical Thinking

Answer 1 The notation $b \mid a$ expresses a relationship between the integers a and b . It states that b divides a (provided $b \neq 0$), meaning a can be written as $a = bq$ for some integer q .

On the other hand, a/b is a rational number with numerator a and denominator b ; it represents an arithmetic operation (division) and does not assert a divisibility relationship between a and b .

Answer 2

(a) **False.**

Proof: By the definition of divisibility, $b \mid a$ means $a = bq$ for some integer q and $b \neq 0$. $0 \mid 7$ means there exists an integer q such that $7 = 0 \cdot q$. But no such integer exists. Therefore, 0 does not divide 7.

(b) **True.**

Proof: By the definition of divisibility, $9 \mid 0$ means there exists an integer q such that $0 = 9 \cdot q$. Pick $q = 0$, then $0 = 9 \cdot 0$. Therefore, 9 divides 0.

(c) **False.**

Proof: By the definition of divisibility, $b \mid a$ means $a = bq$ for some integer q and $b \neq 0$. In $0 \mid 0$, we have $b = 0$, which makes the definition inapplicable. Therefore, 0 does not divide 0.

(d) **True.**

Proof: By the definition of divisibility, $1 \mid 1$ means there exists an integer q such that $1 = 1 \cdot q$. Pick $q = 1$, then $1 = 1 \cdot 1$. Therefore, 1 divides 1.

(e) **False.**

Proof: By the definition of divisibility, $7 \mid 44$ means there exists an integer q such that $44 = 7 \cdot q$. The prime factorization of 44 is $44 = 2 \cdot 2 \cdot 11$. Since 44 does not have 7 in its prime factors, there is no integer q such that $44 = 7 \cdot q$. Therefore, 7 does not divide 44.

(f) **True.**

Proof: By the definition of divisibility, $7 \mid (-42)$ means there exists an integer q such that $-42 = 7 \cdot q$. Pick $q = -6$, then $-42 = (-6) \cdot 7$. Therefore, 7 divides -42 .

(g) **True.**

Proof: By the definition of divisibility, $(-7) \mid 49$ means there exists an integer q such that $49 = (-7) \cdot q$. Pick $q = -7$, then $49 = (-7) \cdot (-7)$. Therefore, -7 divides 49.

(h) **True.**

Proof: By the definition of divisibility, $(-7) \mid (-56)$ means there exists an integer q such that $-56 = (-7) \cdot q$. Pick $q = 8$, then $-56 = (-7) \cdot 8$. Therefore, -7 divides -56 .

(i) **True.**

Proof: We want to show that for all $n \in \mathbb{Z}$, $1 \mid n$. By the definition of divisibility, $1 \mid n$ means for all $n \in \mathbb{Z}$ there exists a q such that $n = 1 \cdot q$. Let $q = n$, then $n = 1 \cdot n = n$. Therefore, $(\forall n \in \mathbb{Z})[1 \mid n]$.

(j) **True.**

Proof: By the definition of divisibility, $n \mid 0$ means for all $n \in \mathbb{N}$, there exists a q such that $0 = n \cdot q$. Let $q = 0$, then $0 = n \cdot 0 = 0$. Therefore, $(\forall n \in \mathbb{N})[n \mid 0]$.

(k) **False.**

Proof: $n \mid 0$ means for all $n \in \mathbb{Z}$, there exists a q such that $0 = n \cdot q$. By the definition of divisibility, $b \mid a$ means $a = bq$ with q an integer and $b \neq 0$. If we let n range over the integers, we have the possibility of n being 0, which makes the definition inapplicable. Therefore, $(\forall n \in \mathbb{Z})[n \mid 0]$ is false.

Answer 3 For any integers a, b, c, d with $a \neq 0$:

(a) **Claim:** $a \mid 0$ and $a \mid a$.

Proof: By the definition of divisibility, $a \mid 0$ means there exists an integer q such that $0 = a \cdot q$. Let $q = 0$; since $a \neq 0$, the divisibility definition holds and $0 = a \cdot 0 = 0$. For $a \mid a$, let $q = 1$, then $a = a \cdot 1$. Therefore, $a \mid 0$ and $a \mid a$.

(b) **Claim:** $a \mid 1$ if and only if $a = \pm 1$.

Proof:

(*Forward:*) Assume $a \mid 1$, which means $1 = aq$. Then $1 = 1 \cdot 1$ or $(-1) \cdot (-1)$. That means $a = 1$ and $q = 1$, or $a = -1$ and $q = -1$. In both cases, a is either 1 or -1 . Therefore, if $a \mid 1$, then $a = \pm 1$.

(*Backward:*) Assume $a = \pm 1$. If $a = 1$, fix $q = 1$, then $1 = a \cdot q = 1 \cdot 1 = 1$, so $a \mid 1$. If $a = -1$, fix $q = -1$, then $1 = a \cdot q = (-1) \cdot (-1) = 1$, so $a \mid 1$.

Hence, by the implication and the converse being true, $a \mid 1$ if and only if $a = \pm 1$.

- (c) **Claim:** If $a \mid b$ and $c \mid d$, then $ac \mid bd$ (for $c \neq 0$).

Proof: Assume $a \mid b$ and $c \mid d$. Then there exist integers m and n such that $b = ma$ and $d = nc$. Substituting yields:

$$bd = ma \cdot nc = mnc = mnac$$

Let $mn = k \in \mathbb{Z}$, then $bd = kac$, which means ac divides bd . Therefore, if $a \mid b$ and $c \mid d$, then $ac \mid bd$.

- (d) **Claim:** If $a \mid b$ and $b \mid c$, then $a \mid c$ (for $b \neq 0$).

Proof: Assume $a \mid b$ and $b \mid c$. Then there exist integers m and n such that $b = am$ and $c = bn$. Substituting gives:

$$c = bn = (am)n = a(mn)$$

Since $mn \in \mathbb{Z}$, a divides c . Therefore, if $a \mid b$ and $b \mid c$, then $a \mid c$.

- (e) **Claim:** $[a \mid b \text{ and } b \mid a]$ if and only if $a = \pm b$.

Proof:

(Forward:) Assume $a \mid b$ and $b \mid a$. That means there exist integers q, r such that $b = qa$ and $a = rb$. For that equality to be true, qr has to multiply to 1. That means q, r are each equal to -1 or 1 . If q and $r = -1$, then $a = -b$. If q and $r = 1$, then $a = b$. Therefore, if $a \mid b$ and $b \mid a$, then $a = \pm b$.

(Backward:) If $a = b$, then $b = qa = 1 \cdot b$, so there exists an integer $q = 1$ such that $b = qa$. It follows that $a = b = rb = 1 \cdot b$, so there exists an integer $r = 1$ such that $a = rb$. Thus, $a \mid b$ and $b \mid a$. If $a = -b$, then $b = qa = (-1)(-b)$, so there exists an integer $q = -1$ such that $b = qa$. It follows that $a = -b = rb = (-1) \cdot b$, so there exists an integer $r = -1$ such that $a = rb$. Thus, $a \mid b$ and $b \mid a$.

Because the implication and the converse are true, $[a \mid b \text{ and } b \mid a]$ if and only if $a = \pm b$.

- (f) **Claim:** If $a \mid b$ and $b \neq 0$, then $|a| \leq |b|$.

Proof: Assume $a \mid b$ and $b \neq 0$. There exists an integer $q \neq 0$ such that $b = qa$. If $|q| = 1$, then $|b| = |a|$. If $|q| > 1$, then $|a| = \frac{|b|}{|q|}$, which means $|a| < |b|$. Therefore, if $a \mid b$ and $b \neq 0$, then $|a| \leq |b|$.

- (g) **Claim:** If $a \mid b$ and $a \mid c$, then $a \mid (bx + cy)$ for any integers x, y .

Proof: Assume $a \mid b$ and $a \mid c$. There exist integers p, q such that $b = pa$ and $c = qa$. Let x, y be any integers:

$$bx + cy = (pa)x + (qa)y = a(px + qy)$$

That means a divides $bx + cy$. Therefore, if $a \mid b$ and $a \mid c$, then $a \mid (bx + cy)$ for any integers x, y .

ANSWERS TO OPTIONAL PROBLEMS

Answer 1 Claim: Let $n > 1$ be a natural number. If n has the property that for all integers a, b , whenever $n \mid ab$, then $n \mid a$ or $n \mid b$, then n must be prime.

Proof: Assume for contradiction that $n > 1$ possesses this property but is composite.

Since n is composite, there exist integers a and b such that $n = ab$ with $1 < a < n$ and $1 < b < n$.

Because $n = ab$, n divides ab (as $n = 1 \cdot ab$). By our hypothesis, n must divide a or n must divide b .

If $n \mid a$, then since a is a positive integer, we must have $n \leq a$, which contradicts $a < n$. Similarly, if $n \mid b$, we must have $n \leq b$, which contradicts $b < n$.

In either case, we reach a contradiction. Therefore, n cannot be composite and must be prime.

Answer 2 Euclid's Lemma: Let p be a prime number and $a, b \in \mathbb{Z}$. If $p \mid ab$, then $p \mid a$ or $p \mid b$.

Proof: Let p be a prime number and suppose $p \mid ab$. We consider two cases: $p \mid a$ or $p \nmid a$.

If $p \mid a$, the conclusion holds immediately.

Now suppose $p \nmid a$. Since p is prime, its only positive divisors are 1 and p . Because p does not divide a , the greatest common divisor of a and p is 1, that is, $\gcd(a, p) = 1$.

By Bézout's Identity, there exist integers x and y such that:

$$ax + py = 1$$

Multiplying both sides of this equation by b yields:

$$abx + pby = b$$

Since $p \mid ab$, there exists an integer k such that $ab = pk$. Substituting $ab = pk$ into the equation gives:

$$(pk)x + pby = b \implies p(kx + by) = b$$

Since $kx + by \in \mathbb{Z}$, it follows by definition that $p \mid b$.

Therefore, whenever $p \mid ab$, $p \mid a$ or $p \mid b$.