1. Express as concisely and accurately as you can the relationship between \( b \mid a \) and \( a/b \).

**SOLUTION**

\( a/b \) is a notation that denotes the rational number \( a \) divided by \( b \). \( b \mid a \) denotes the relation that \( b \) divides \( a \), i.e., there is an integer \( q \) such that \( a = qb \). In the case where \( b \mid a \), then \( q = a/b \).

Thus, \( b \mid a \) iff \( a/b \) is an integer.

2. Determine whether each of the following is true or false and prove your answer. (You saw these questions in the in-lecture quiz, so the first part is a repeat, except that now you should know the right answers.) The focus of this assignment is to prove each of your answers.

(a) \(0 \mid 7\)  
(b) \(9 \mid 0\)  
(c) \(0 \mid 0\)  
(d) \(1 \mid 1\)

(e) \(7 \mid 44\)  
(f) \(7 \mid (−42)\)  
(g) \((-7) \mid 49\)  
(h) \((-7) \mid (−56)\)

(i) \((\forall n \in \mathbb{Z})[1 \mid n]\)  
(j) \((\forall n \in \mathbb{N})[n \mid 0]\)  
(k) \((\forall n \in \mathbb{Z})[n \mid 0]\)

**SOLUTION**

(a) False. \(a \mid b\) includes the requirement \( a \neq 0 \).

(b) True. \(0 = 0 \times 9\), so \((\exists q)(0 = q.9)\).

(c) False. \(a \mid b\) includes the requirement \( a \neq 0 \).

(d) True. \(1 = 1 \times 1\), so \((\exists q)(1 = q.1)\).

(e) False. \(−(\exists q)(44 = q.7)\).

(f) True. \(-42 = (−6) \times 7\).

(g) True. \(49 = (−7) \times (−7)\).

(h) True. \(-56 = 8 \times (−7)\).

(i) True. For any \(n \in \mathbb{Z}\), \(n = n.1\).

(j) True. For any \(n \in \mathbb{Z}\), \(0 = 0.n\).

(k) False. \(n \mid 0\) includes the requirement \( n \neq 0 \).

3. Prove all the parts of the theorem in the lecture, giving the basic properties of divisibility. Namely, show that for any integers \(a, b, c, d\), with \(a \neq 0\):

(a) \(a \mid 0\), \(a \mid a\);

(b) \(a \mid 1\) if and only if \(a = \pm 1\);

(c) if \(a \mid b\) and \(c \mid d\), then \(ac \mid bd\) (for \(c \neq 0\));

(d) if \(a \mid b\) and \(b \mid c\), then \(a \mid c\) (for \(b \neq 0\));

(e) \([a \mid b\) and \(b \mid a]\) if and only if \(a = \pm b\);

(f) if \(a \mid b\) and \(b \neq 0\), then \(|a| \leq |b|\);

(g) if \(a \mid b\) and \(a \mid c\), then \(a \mid (bx + cy)\) for any integers \(x, y\).

**SOLUTION**

(a) Since \(0 = 0 \times a\), it is the case that \((\exists q \in \mathbb{Z})[0 = q.a]\), so by definition \(a \mid 0\). Since \(a = 1 \times a\), it is the case that \((\exists q \in \mathbb{Z})[a = q.a]\), so by definition \(a \mid a\).
(b) If $a = \pm 1$, then $a|1$ follows immediately from the definition (namely $(\exists q \in \mathbb{Z})[1 = q.a]$). Conversely, of $a|1$, then for some $q$, $1 = q.a$, so $|1| = |q.a| = |q||a|$, so $|q| = |a| = 1$, so in particular $a = \pm 1$.

(c) By the assumption, there are integers $q,r$ such that $b = q.a$ and $d = r.c$. Hence $bd = (qa)(rc) = (qr)(ac)$, which shows that $ac|bd$.

(d) By the assumption, there are integers $q,r$ such that $b = q.a$ and $c = r.b$. Hence $c = rb = r(qa) = (rq)a$, which shows that $a|c$.

(e) If $a = \pm b$, then $a = qb$ and $b = ra$, where $q,r$ are each one of $\pm 1$. So $a|b$ and $b|a$. Conversely, if there are $q,r$ such that $b = qa$ and $a = rb$, then $a = rb = rqa$, so (canceling the $a$) $1 = rq$, which implies that $q = r = 1$ or $q = r = -1$, so $a = \pm b$.

(f) If $b = qa$, then $|b| = |qa| = |q|.|a|$. So, as $|q| \geq 1$, $|a| \leq |b|$.

(g) If $b = qa$ and $c = ra$, then $bx + cy = bqa + cra = (bq + cr)a$, proving that $a|(bx + cy)$

4. Prove that if $p$ is prime, then $\sqrt{p}$ is irrational. (You can assume that if $p$ is prime, then whenever $p$ divides a product $ab$, $p$ divides at least one of $a,b$.)

**SOLUTION**

We prove the result by contradiction. Suppose $\sqrt{p}$ were rational, say $\sqrt{p} = m/n$, where $m,n$ are natural numbers. We may assume (without loss of generality) that $m,n$ have no common factors.

Then, squaring, $p = m^2/n^2$, so $m^2 = pn^2$. Thus $p|m^2$.

Since $p$ is prime, it follows that $p|m$. Hence $m = pq$ for some natural number $q$.

Substituting $m = pq$ in the equation $m^2 = pn^2$, we get $(pq)^2 = pn^2$, so $p^2q^2 = pn^2$, which simplifies to $pq^2 = n^2$. Thus $p|n^2$.

Hence, as $p$ is prime, $p|n$. Thus $p$ is a common factor of $m,n$, contrary to the choice of $m,n$.

This completes the proof.