Sample homework solutions for 1.2

Jim Brown

4. a. Prove that if $a|x$ and $b|y$, then $ab|xy$.

Proof: Using the defintion of divisbility, we see that there exists $s, t \in \mathbb{Z}$ so that $as = x$ and $bt = y$. Multiplying these together we have $abst = xy$, i.e., $ab|xy$. ■

b. Prove that if $d = \gcd(a, b)$, then $\gcd\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

Proof: The fact that $d = \gcd(a, b)$ tells us that $d|a$ and $d|b$, i.e., there exists $s, t \in \mathbb{Z}$ so that $ds = a$ and $dt = b$. In light of this, what we are trying to show is that $\gcd(s, t) = 1$ as $s = \frac{a}{d}$ and likewise for t. Using that d is the greatest common divisor of a and b we have that there exists $m, n \in \mathbb{Z}$ so that $d = am + bn$. Dividing each side by d we obtain $1 = sm + tn$. Now apply Corollary 2.4 to conclude that $\gcd(s, t) = 1$. ■

8. Suppose $a, b, n \in \mathbb{N}$, $\gcd(a, n) = 1$, and $\gcd(b, n) = 1$. Prove or give a counterexample: $\gcd(ab, n) = 1$.

Proof: We prove this by contradiction. Suppose that $\gcd(ab, n) = d$ and $d > 1$. The fundamental theorem of arithmetic shows that there exists a prime p so that $p|d$ since $d > 1$. In particular, since $d|n$ and $d|ab$, we have that $p|n$ and $p|ab$. Using Proposition 2.5 we see that $p|ab$ implies that $p|a$ or $p|b$. However, this would give that either $p|\gcd(a, n)$ or $p|\gcd(b, n)$, a contradiction as they are both assumed to be 1. Thus it must be that $d = 1$. ■

9. Prove that if p is prime and $p|(a_1 \dots a_n)$, then $p|a_j$ for some j, $1 \le j \le n$.

Proof: We prove this statement by induction. The base case of $n = 2$ says that if $p|ab$ then $p|a$ or $p|b$. This is precisely the statement of Proposition 2.5 so the base case is true. Now suppose that if $p|(a_1 \dots a_k)$ then $p|a_j$ for some j, $1 \le j \le k$. (our induction hypothesis) Suppose that $p|(a_1 a_2 \dots a_k a_{k+1})$. In particular, we can group the term $a_1 \dots a_k a_{k+1}$ as $(a_1 \dots a_k)a_{k+1}$ and use Proposition 2.5 again to conclude that $p|(a_1 \dots a_k)$ or $p|a_{k+1}$. If $p|a_{k+1}$ we are done. If not, $p|(a_1 \dots a_k)$ and we apply our induction hypothesis to conclude that $p|a_j$ for some j, $1 \le j \le k$. Thus, by induction the statement holds for all n. ■

11. Prove that there are no integers m, n so that $\left(\frac{m}{n}\right)^2 = 2$.

Proof: Suppose that there are integers m, n so that $\left(\frac{m}{n}\right)^2 = 2$. We may assume that $\gcd(m, n) = 1$ for if not we could cancel it out. This is just saying we put the fraction in lowest terms. We can rewrite our equality as

$$m^2 = 2n^2.$$

In particular, it must be the case that $2|m^2$. Applying Proposition 2.5 we see that $2|m$, i.e., m is even. Thus there exists an integer s so that $m = 2s$. We can again rewrite our equation as

$$(2s)^2 = 2n^2.$$

In particular, we have that $2s^2 = n^2$. Applying the same argument as above we obtain that $2|n$. This is a contradiction though as we assumed $\gcd(m, n) = 1$ and we have just shown that $2|m$ and $2|n$. Thus it must be the case that there are no such integers m and n. ■