Solutions to Homework #9

1. Section 3.2, Problem 3 (8 points)
Let $a, b, s, t, u, v \in \mathbb{Z}$ be integers such that $sa + tb = 21$ and $ua + vb = 10$. Prove that $\gcd(a, b) = 1$.

Proof. We have

$$(s - 2u)a + (t - 2v)b = (sa + tb) - 2(ua + vb) = 21 - 2(10) = 1.$$

Since $s - 2u, t = 2v \in \mathbb{Z}$, we have that $\gcd(a, b) = 1$. QED

Note: that last conclusion is by Theorem 3.2.3. Or, if you object that Theorem 3.2.3 is only stated for $a, b \in \mathbb{N}$ — in fact, it is true for all $a, b \in \mathbb{Z}$ — then here's a proof, essentially just quoting the end of the proof of Theorem 3.2.3:

If $d \in \mathbb{N}$ divides both a and b, i.e., if there exist integers $k, \ell \in \mathbb{Z}$ such that $a = dk$ and $b = d\ell$, then $1 = dk(s - 2u) + d\ell(t - 2v) = dn$ where $n = k(s - 2u) + \ell(t - 2v) \in \mathbb{Z}$. Thus, 1 is divisible by $d \in \mathbb{N}$, and since the only divisors of 1 are ± 1, we have $d = 1$. That is, the *only* common divisor of a and b is 1, so the *greatest* common divisor of a and b is also 1.

---

2. Section 3.2, Problem 9 (10 points)
Let $a, b \in \mathbb{Z} \setminus \{0\}$ be nonzero integers. Prove that $\gcd(a, b) = 1$ if and only if $\gcd(a, a + b) = 1$.

Proof (Method 1). Given $a, b \in \mathbb{Z} \setminus \{0\}$ arbitrary.
($\Longrightarrow$): Assume $\gcd(a, b) = 1$. For any common divisor $d \in \mathbb{N}$ of both a and $a + b$, there are integers $m, n \in \mathbb{Z}$ such that $a = md$ and $a + b = nd$. Therefore, $b = (a + b) - a = (n - m)d$ is also divisible by d. So d is a common divisor of both a and b. Since $\gcd(a, b) = 1$, it follows that $d = 1$. Because this was true for all such d, we have that $\gcd(a, a + b) = 1$.

($\Longleftarrow$): Assume $\gcd(a + b, b) = 1$. For any common divisor $d \in \mathbb{N}$ of both a and b, there are integers $m, n \in \mathbb{Z}$ such that $a = md$ and $b = nd$. Therefore, $a + b = (m + n)d$ is also divisible by d.
So d is a common divisor of both a and $a + b$. Since $\gcd(a, a + b) = 1$, it follows that $d = 1$. Because this was true for all such d, we have that $\gcd(a, b) = 1$. QED

Proof (Method 2). Given $a, b \in \mathbb{Z} \setminus \{0\}$:
($\Longrightarrow$): By Theorem 3.2.5 [extended to all integers], there are integers $m, n \in \mathbb{Z}$ such that $ma + nb = 1$. Thus, $(m - n)a + n(a + b) = ma + nb = 1$. Since $m - n$ and n are integers, it follows from Theorem 3.2.5 that $\gcd(a, a + b) = 1$.
($\Longleftarrow$) By Theorem 3.2.5 [extended to all integers], there are integers $m, n \in \mathbb{Z}$ such that $ma + n(a + b) = 1$. Thus, $(m + n)a + nb = ma + n(a + b) = 1$. Since $m + n$ and n are integers, it follows from Theorem 3.2.5 that $\gcd(a, b) = 1$. QED

---

3. Section 3.3, Problem 3 (12 points)
Prove Corollary 3.3.5: For any $m, n \in \mathbb{N}$, we have $mn = \gcd(m, n) \operatorname{lcm}(m, n)$

Proof. Let $p_1, \ldots, p_k$ be all of the distinct prime numbers that divide m or n. Then there are nonnegative integers $e_1, \ldots, e_k, f_1, \ldots, f_k \geq 0$ such that

$$m = p_1^{e_1} \cdots p_k^{e_k} \quad \text{and} \quad n = p_1^{f_1} \cdots p_k^{f_k}.$$

(Note that it's possible that not all of the primes $p_1, \ldots, p_k$ divide m, and similarly for n, so that some of the exponents e_i, f_i may be 0.)

Lemma. For any integers e, f we have $\min\{e, f\} + \max\{e, f\} = e + f$.

Proof of Lemma. Without loss of generality, we have $e \leq f$. Thus, $\min\{e, f\} = e$ and $\max\{e, f\} = f$. The conclusion of the Lemma follows immediately. QED Lemma

By Corollary 3.3.4, we have

$$\gcd(m,n) = p_1^{\min\{e_1,f_1\}} \cdots p_1^{\min\{e_k,f_k\}} \quad \text{and} \quad \operatorname{lcm}(m,n) = p_1^{\max\{e_1,f_1\}} \cdots p_1^{\max\{e_k,f_k\}}.$$

Thus, by the Lemma above,

$$\begin{aligned} mn &= p_1^{e_1+f_1} \cdots p_k^{e_k+f_k} = p_1^{\min\{e_1,f_1\}+\max\{e_1,f_1\}} \cdots p_k^{\min\{e_k,f_k\}+\max\{e_k,f_k\}} \\ &= \left(p_1^{\min\{e_1,f_1\}} \cdots p_k^{\min\{e_k,f_k\}}\right) \cdot \left(p_1^{\max\{e_1,f_1\}} \cdots p_k^{\max\{e_k,f_k\}}\right) = \gcd(m,n) \operatorname{lcm}(m,n). \end{aligned}$$

QED

Note: You don't have to state the thing about $\min\{e,f\} + \max\{e,f\} = e+f$ as being its own Lemma. I just found that to be the easiest way to say it, for clarity.

---

4. Section 3.3, Problem 6 (10 points)

Prove that for every $n \in \mathbb{N}$, we have $\dfrac{(3n)!}{3^n} \in \mathbb{N}$

Proof. By induction on $n \geq 1$.

Base case: $n = 1$. Then $(3n)! = 3! = 6$, and $3^n = 3$, and so $\dfrac{(3n)!}{3^n} = \dfrac{6}{3} = 2 \in \mathbb{N}$.

Inductive Step: Assume the conclusion is true for some particular $n \in \mathbb{N}$; we will prove it for $n+1$. Let $m = \dfrac{(3n)!}{3^n} \in \mathbb{N}$.

Then $\dfrac{(3(n+1))!}{3^{n+1}} = \dfrac{3(n+1)\cdot(3n+2)\cdot(3n+1)}{3} \cdot \dfrac{(3n)!}{3^n} = (n+1)\cdot(3n+2)\cdot(3n+1)\cdot m$ is a product of positive integers, and hence is a positive integer, as desired. QED

---

5. Section 3.3, Problem 10 (14 points)

Let $a, d \in \mathbb{N}$. Prove that $d|a$ if and only if $d^2|a^2$.

Proof. Given $a, d \in \mathbb{N}$:

($\Longrightarrow$): By assumption, there is an integer $k \in \mathbb{Z}$ such that $a = dk$. Then $a^2 = (d^2)(k^2)$, and hence because $k^2 \in \mathbb{Z}$ as well, we have $d^2|a^2$.

($\Longleftarrow$): By assumption, there is an integer $m \in \mathbb{Z}$ such that $a^2 = md^2$. Since $a, d > 0$, we have $m > 0$, so $m \in \mathbb{N}$.

Let $p_1, \ldots, p_k$ be all of the distinct prime numbers that divide a or d or m. Then there are nonnegative integers $e_1, \ldots, e_k, f_1, \ldots, f_k, g_1, \ldots, g_k \geq 0$ such that

$$a = p_1^{e_1} \cdots p_k^{e_k}, \quad d = p_1^{f_1} \cdots p_k^{f_k}, \quad \text{and} \quad m = p_1^{g_1} \cdots p_k^{g_k}.$$

Plugging these values in the equation $a^2 = md^2$, we obtain

$$p_1^{2e_1} \cdots p_k^{2e_k} = p_1^{2f_1+g_1} \cdots p_k^{2f_k+g_k}.$$

By the uniqueness of prime factorizations, then, we have $2e_i = 2f_i + g_i$ for every $i = 1, \ldots, k$, and hence $g_i = 2(e_i - f_i)$ for each i.

For each i, let $h_i = e_i - f_i \in \mathbb{Z}$. We have $h_i = g_i/2 \geq 0$, so we may define

$$n = p_1^{h_1} \cdots p_k^{h_k} \in \mathbb{N},$$

which satisfies

$$nd = \left(p_1^{h_1} \cdots p_k^{h_k}\right) \cdot \left(p_1^{f_1} \cdots p_k^{f_k}\right) = p_1^{e_1} \cdots p_k^{e_k} = a,$$

since $h_i + f_i = e_i$ for each $i = 1, \ldots k$. Thus, $d|a$. QED

---

6. Section 3.3, Problem 11 (16 points)

Prove that for any $n \in \mathbb{N}$, we have that $\sqrt{n}$ either is an integer or is irrational.

Proof, Method 1. Suppose that $\sqrt{n}$ is rational; we will prove that it is an integer.

By assumption, there are integers $a, b \in \mathbb{Z}$ such that $\sqrt{n} = a/b$; since $\sqrt{n} > 0$ by definition of square root (and the fact that $n > 0$), we may assume that $a/b > 0$, i.e., that $a/b \in \mathbb{N}$. Cancelling any minus signs, we may further assume that $a, b \in \mathbb{N}$.
Multiplying by b and squaring both sides, then, we have $a^2 = b^2 n$. Thus, we have $a, b \in \mathbb{N}$ with $b^2 | a^2$. By Problem 5 on this assignment (i.e., Section 3.3, Problem 10), it follows that $b|a$.
That is, there is an integer $m \in \mathbb{Z}$ such that $a = bm$. Therefore, $\sqrt{n} = a/b = (bm)/b = m \in \mathbb{Z}$ is an integer. QED

_______ _______ _______ _______ _______ _______ _______

Proof, Method 2. Suppose that $\sqrt{n}$ is rational; we will prove that it is an integer.
By assumption, there are integers $a, b \in \mathbb{Z}$ such that $\sqrt{n} = a/b$; since $\sqrt{n} > 0$ by definition of square root (and the fact that $n > 0$), we may assume that $a/b > 0$, i.e., that $a/b \in \mathbb{N}$.
Let $p_1, \ldots, p_k$ be all of the distinct prime numbers that divide n or a or b. Then there are nonnegative integers $e_1, \ldots, e_k, f_1, \ldots, f_k, g_1, \ldots, g_k \geq 0$ such that

$$a = p_1^{e_1} \cdots p_k^{e_k}, \quad b = p_1^{f_1} \cdots p_k^{f_k}, \quad \text{and} \quad n = p_1^{g_1} \cdots p_k^{g_k}.$$

Since $\sqrt{n} = a/b$, multiplying by b and squaring gives $b^2 n = a^2$, and hence

$$p_1^{2f_1+g_1} \cdots p_k^{2f_k+g_k} = p_1^{2e_1} \cdots p_k^{2e_k}.$$

By the uniqueness of prime factorizations, then, we have $2f_i + g_i = 2e_i$ for every $i = 1, \ldots, k$, and hence $g_i = 2(e_i - f_i)$.
For each i, let $h_i = e_i - f_i \in \mathbb{Z}$. We have $h_i = g_i/2 \geq 0$, so we may define

$$m = p_1^{h_1} \cdots p_k^{h_k} \in \mathbb{N},$$

which satisfies

$$m = p_1^{e_1-f_1} \cdots p_k^{e_k-f_k} = \frac{p_1^{e_1} \cdots p_k^{e_k}}{p_1^{f_1} \cdots p_k^{f_k}} = \frac{a}{b} = \sqrt{n}.$$

Thus $\sqrt{n} = m \in \mathbb{N}$ is an integer. QED