Homework 5 Solutions

via Gradescope

- Failure to submit homework correctly will result in zeroes.
- Handwritten homework is OK. You do not have to type up your work.
- Problems assigned from the textbook are from the 5^{th} edition.
- No late homework accepted. Lateness due to technical issues will not be excused.

1. (3 points) Section 4.8 #8.

   Solution: #8.

   Conjecture. $\sqrt{4} \notin \mathbb{Q}$.

   Disproof. $\sqrt{4} = \sqrt{2(2)} = \sqrt{2}(\sqrt{2}) = 2 \in \mathbb{Z} \subseteq \mathbb{Q}$ so $\sqrt{4} \in \mathbb{Q}$. □

2. (3 points) Prove or disprove the following conjecture.

   Conjecture. *$xy \in \mathbb{R} - \mathbb{Q}$ for any $x, y \in \mathbb{R} - \mathbb{Q}$.*

   Disproof. Choose $x = y = \sqrt{2} \in \mathbb{R} - \mathbb{Q}$ such that

   $$xy = \sqrt{2}(\sqrt{2}) = \sqrt{2(2)} = \sqrt{4} = 2 \in \mathbb{Z} \subseteq \mathbb{Q}$$

   so $xy \in \mathbb{Q}$. □

3. (6 points) Provided the Pythagorean Theorem 4.8.1, $\sqrt{2} \notin \mathbb{Q}$:

   (a) Prove that $\sqrt{6} \notin \mathbb{Q}$ using Proposition 4.7.4 and Euclid's lemma.

   (b) Prove that $\sqrt{2} + \sqrt{3} \notin \mathbb{Q}$ using the previous part.

   Proposition (4.7.4)**.** *$n^2 \in 2\mathbb{Z}$ implies $n \in 2\mathbb{Z}$ for any $n \in \mathbb{Z}$.*

   Lemma (Euclid's lemma)**.** *Let p be prime. Let $a, b \in \mathbb{Z}$ and $a > 1$ and $b > 1$. If $p \mid ab$ and $p \nmid a$, then $p \mid b$.*

   Solution:

(a) *Proof.* Suppose $\sqrt{6} \in \mathbb{Q}$. There exist $m \in \mathbb{Z}$ and $n \in \mathbb{Z} - \{0\}$ such that m, n are relatively prime and $\sqrt{6} = \frac{m}{n}$.

$$\begin{aligned} \sqrt{6} &= \frac{m}{n} \\ 6 &= \frac{m^2}{n^2} \\ 6n^2 &= m^2 \\ 2(3n^2) &= m^2 \end{aligned}$$

$3n^2 \in \mathbb{Z}$ since $\mathbb{Z}$ is closed under products, so $m^2 \in 2\mathbb{Z}$. $m \in 2\mathbb{Z}$ via Proposition 4.7.4. $m = 2k_1$ for some integer $k_1 \in \mathbb{Z}$.

$$\begin{aligned} 6n^2 &= m^2 = (2k_1)^2 = 4k_1^2 \\ 3n^2 &= 2k_1^2 \end{aligned}$$

$k_1^2 \in \mathbb{Z}$ since $\mathbb{Z}$ is closed under products, so $2 \mid (3n^2)$. $2 \mid (3n^2)$ and 2 is prime but $2 \nmid 3$ so $2 \mid n^2$ via Euclid's lemma. $n^2 \in 2\mathbb{Z}$ implies $n \in 2\mathbb{Z}$ via Proposition 4.7.4. $n = 2k_2$ for some integer $k_2 \in \mathbb{Z}$. However now m, n have a common factor of $2 > 1$, which contradicts that m, n are relatively prime to write in reduced form, $\frac{m}{n} \in \mathbb{Q}$.

Thus $\sqrt{6} \notin \mathbb{Q}$. $\square$

(b) *Proof.* Suppose $\sqrt{2} + \sqrt{3} \in \mathbb{Q}$. There exist $m \in \mathbb{Z}$ and $n \in \mathbb{Z} - \{0\}$ such that $\sqrt{2} + \sqrt{3} = \frac{m}{n}$.

$$\begin{aligned} \sqrt{2} + \sqrt{3} &= \frac{m}{n} \\ (\sqrt{2} + \sqrt{3})^2 &= \left(\frac{m}{n}\right)^2 \\ 2 + 3 + 2\sqrt{6} &= \frac{m^2}{n^2} \\ 2\sqrt{6} &= \frac{m^2}{n^2} - 5 \\ \sqrt{6} &= \frac{m^2 - 5n^2}{2n^2} \end{aligned}$$

$m^2 - 5n^2 \in \mathbb{Z}$ since $\mathbb{Z}$ is closed under products and differences. $2n^2 \in \mathbb{Z}$ since $\mathbb{Z}$ is closed under products. $2 \neq 0$ and $n \neq 0$ since $n \in \mathbb{Z} - \{0\}$, so $2n^2 \neq 0$ via Zero Product Property. Thus $\sqrt{6} \in \mathbb{Q}$ but this contradicts $\sqrt{6} \notin \mathbb{Q}$ from the previous part. Therefore $\sqrt{2} + \sqrt{3} \notin \mathbb{Q}$. $\square$

4. (6 points) Section 4.10 #12, 15.

Solution: #12.

$48 = 3(16) = (2^4)3$ and $54 = 2(27) = 2(3^3)$ so $\gcd(48, 54) = 2(3) = 6$.

#15. Following the Euclidean algorithm and written in the form of the Quotient-Remainder theorem:

$$\begin{aligned} 10933 &= 832(13) + 117 \\ 832 &= 117(7) + 13 \\ 117 &= 13(9) + 0 \end{aligned}$$

so $\gcd(10933, 832) = \gcd(832, 117) = \gcd(117, 13) = \gcd(13, 0) = 13$.

5. (6 points) Section 4.10 #22, 24.

Definition. Let $a, b \in \mathbb{Z}$, not both zero. $d \in \mathbb{Z}$ is the *greatest common divisor* of a and b, denoted $\gcd(a, b)$, if and only if

(1) $d \mid a$ and $d \mid b$

(2) For any $c \in \mathbb{Z}$, $c \mid a$ and $c \mid b$ implies $c \leq d$.

Definition. $a, b \in \mathbb{Z}$ are *relatively prime* if and only if $\gcd(a, b) = 1$.

Solution: #22.

Theorem. $a \mid b$ *if and only if* $\gcd(a, b) = a$ *for any* $a, b \in \mathbb{Z}^+$.

Proof. Let $a, b \in \mathbb{Z}^+$.

Case 1: Suppose $a \mid b$. $1 \in \mathbb{Z}$ such that $a = a(1)$ so $a \mid a$. So $a \mid a$ and $a \mid b$ and a is a common divisor of a and b. $a \leq \gcd(a, b)$ via definition of greatest common divisor. Provided $d := \gcd(a, b)$, $d \mid a$ and $d \mid b$. $d \mid a$ via specialization, so $d \leq a$ via Theorem 4.4.1 and $\gcd(a, b) \leq a$. Since $a \leq \gcd(a, b)$ and $\gcd(a, b) \leq a$, $a = \gcd(a, b)$.

Case 2: Suppose $\gcd(a, b) = a$. So $a \mid b$ and $a \mid a$. Also if $c \mid a$ and $c \mid b$ then $c \leq a$ for any $c \in \mathbb{Z}$. $a \mid b$ via specialization.

Thus $a \mid b$ if and only if $\gcd(a, b) = a$ for any $a, b \in \mathbb{Z}^+$. □

#24.

Lemma (4.10.2)**.** *For any* $a, b \in \mathbb{Z}$ *not both zero and* $q, r \in \mathbb{Z}$*,* $a = bq + r$ *implies* $\gcd(a, b) = \gcd(b, r)$.

Proof. Let $a, b \in \mathbb{Z}$, not both zero, and $q, r \in \mathbb{Z}$. Suppose $a = bq + r$.

Case 2: Our goal is to show that $\gcd(b, r) \leq \gcd(a, b)$.

(a) Let c be a common divisor of b and r, i.e. $c \mid b$ and $c \mid r$. There exist $k_1, k_2 \in \mathbb{Z}$ such that $b = k_1 c$ and $r = k_2 c$.

$$\begin{aligned} a &= bq + r \\ a &= (k_1 c)q + k_2 c \\ a &= c(k_1 q + k_2) \end{aligned}$$

$k_1 q + k_2 \in \mathbb{Z}$ since $\mathbb{Z}$ is closed under products and sums, so $c \mid a$. $c \mid a$ and $c \mid b$ via conjunction, so c is common divisor of a and b. Thus every common divisor of b and r is a common divisor of a and b.

(b) Since $a \neq 0$ or $b \neq 0$, i.e. a, b are not both zero, a and b have a greatest common divisor. Since every common divisor of b and r is a common divisor of a and b from part (a), the greatest common divisor of b and r is a common divisor of a and b. Thus

$$\gcd(b, r) \leq \gcd(a, b)$$

since $\gcd(a, b)$ is the greatest such divisor.

□

6. (6 points) Section 4.10 #28, 29.

Definition. Let $a, b \in \mathbb{Z} - \{0\}$. $c \in \mathbb{Z}^+$ is the *least common multiple* of a and b, denoted $\operatorname{lcm}(a, b)$, if and only if

(1) $a \mid c$ and $b \mid c$

(2) For any $m \in \mathbb{Z}^+$, $a \mid m$ and $b \mid m$ implies $c \leq m$.

Solution: #28.

(a) $18 = 2(3^2)$ and $12 = (2^2)(3)$ so $\operatorname{lcm}(12, 18) = (2^2)(3^2) = 4(9) = 36$.

(b) $\operatorname{lcm}(2^2 \cdot 3 \cdot 5, 2^3 \cdot 3^2) = (2^3)(3^2)(5) = 360$.

(c) $2800 = 28(100) = (2^2)(7)(2^2)(5^2) = (2^4)(5^2)(7)$ and $6125 = (125)(49) = (5^3)(7^2)$ so

$$\operatorname{lcm}(2800, 6125) = (2^4)(5^3)(7^2) = (2)(5)(4)(25)(2)(49) = (10)(100)(98) = 98000.$$

#29.

Theorem. $\gcd(a, b) = \operatorname{lcm}(a, b)$ *if and only if* $a = b$ *for any* $a, b \in \mathbb{Z}^+$.

Proof. Let $a, b \in \mathbb{Z}^+$.

Case 1: Suppose $a = b$.

(i) $1 \in \mathbb{Z}$ such that $a = a(1)$ and $b = a(1)$, so $a \mid a$ and $a \mid b$. Thus a is a common divisor of a and b, so $a \leq \gcd(a, b)$. $1 \in \mathbb{Z}$ such that $a = b(1)$, so $b \mid a$. $a \mid a$ and $b \mid a$ so $\operatorname{lcm}(a, b) \leq a$. $\operatorname{lcm}(a, b) \leq a$ and $a \leq \gcd(a, b)$, so $\operatorname{lcm}(a, b) \leq \gcd(a, b)$ via transitivity.

(ii) $\gcd(a, b) \mid a$ so $\gcd(a, b) \leq a$ via Theorem 4.4.1. $a \mid \operatorname{lcm}(a, b)$ so $\operatorname{lcm}(a, b) = ka$ for some $k \in \mathbb{Z}$. $\operatorname{lcm}(a, b) > 0$ by definition and $a > 0$ so $k \geq 1 > 0$ via Property T25. $\operatorname{lcm}(a, b) = ka \geq (1)a = a$. $\gcd(a, b) \leq a$ and $a \leq \operatorname{lcm}(a, b)$, so $\gcd(a, b) \leq \operatorname{lcm}(a, b)$ via transitivity.

$\operatorname{lcm}(a, b) \leq \gcd(a, b)$ and $\gcd(a, b) \leq \operatorname{lcm}(a, b)$, so $\gcd(a, b) = \operatorname{lcm}(a, b)$.

$a = b$ implies $\gcd(a, b) = \operatorname{lcm}(a, b)$.

Case 2: Suppose $c := \gcd(a, b) = \operatorname{lcm}(a, b) > 0$.

(i) $c \mid a$ by definition of greatest common divisor, so $c \leq a$ via Theorem 4.4.1. $a \mid c$ by definition of least common multiple, so $a \leq c$ via Theorem 4.4.1. Thus $a = c$.

(ii) $c \mid b$ by definition of greatest common divisor, so $c \leq b$ via Theorem 4.4.1. $b \mid c$ by definition of least common multiple, so $b \leq c$ via Theorem 4.4.1. Thus $b = c$.

$a = b$ via transitivity.

$\gcd(a, b) = \operatorname{lcm}(a, b)$ implies $a = b$.

Therefore $\gcd(a, b) = \operatorname{lcm}(a, b)$ if and only if $a = b$. $\square$

7. (3 points) Section 5.1 #79.

Solution: Recall Euclid's lemma.

Proof. Let $p > 1$ be prime and $r \in \mathbb{Z}$ such that $0 < r < p$.

$\binom{p}{r} \in \mathbb{Z}$ since $\binom{n}{k} \in \mathbb{Z}$ for any $n, k \in \mathbb{Z}$ such that $n \geq k \geq 0$.

Since $p - r = p - r + 0 = p - r + 1 - 1 = p - 1 - (r - 1)$,

$$\binom{p}{r} = \frac{p!}{r!(p-r)!} = \frac{p(p-1)!}{r(r-1)!(p-1-(r-1))!} = \frac{p}{r}\binom{p-1}{r-1}$$
$$r\binom{p}{r} = p\binom{p-1}{r-1}.$$

$\binom{p-1}{r-1} \in \mathbb{Z}$ since $p - 1 > r - 1 \geq 0$, so $p \mid \left(r\binom{p}{r}\right)$. $p > 1$ is prime and $p \nmid r$ since $0 < r < p$, therefore $p \mid \binom{p}{r}$ via Euclid's lemma. $\square$