INTRODUCTION TO PROOFS: HOMEWORK SOLUTIONS

STEVEN HEILMAN

Contents

1. Homework 1

1.1. **Problem 1.** Let $A = \{1, 2, 5\}$ and let $B = \{2, 7\}$. What are: $A \cup B$? $A \cap B$? $A \times B$?

$$A \cup B = \{1, 2, 5, 7\}$$
$$A \cap B = \{2\}$$
$$A \times B = \{(1, 2), (1, 7), (2, 2), (2, 7), (5, 2), (5, 7)\}$$

1.2. **Problem 2.** Let $A = \{x \in \mathbb{N} \colon x \text{ is a multiple of } 6\}$, and let $B = \{x \in \mathbb{N} \colon x \text{ is a multiple of } 15\}$. Let $\mathbb{N} = X$ be the universal set. What are: A^c? $(A^c)^c$? B^c? $A \cup B$? $A \cap B$? $A^c \cup B^c$? $A^c \cap B^c$? $(A \cap B)^c$? $(A \cup B)^c$? $A^c \cup B$? $A \cup B^c$?

Date: May 8, 2012.

$$
\begin{aligned}
A^c &= \{x \in \mathbb{N} \colon x \text{ is not a multiple of } 6\}\\
(A^c)^c &= A = \{x \in \mathbb{N} \colon x \text{ is a multiple of } 6\}\\
B^c &= \{x \in \mathbb{N} \colon x \text{ is not a multiple of } 15\}\\
A \cup B &= \{x \in \mathbb{N} \colon x \text{ is a multiple of } 6, \text{ or } x \text{ is a multiple of } 15\}\\
A \cap B &= \{x \in \mathbb{N} \colon x \text{ is a multiple of } 30\}\\
A^c \cup B^c &= (A \cap B)^c = \{x \in \mathbb{N} \colon x \text{ is not a multiple of } 30\}\\
A^c \cap B^c &= \{x \in \mathbb{N} \colon x \text{ is not a multiple of } 6, \text{ and } x \text{ is not a multiple of } 15\}\\
(A \cap B)^c &= A^c \cup B^c = \{x \in \mathbb{N} \colon x \text{ is not a multiple of } 30\}\\
(A \cup B)^c &= A^c \cap B^c = \{x \in \mathbb{N} \colon x \text{ is not a multiple of } 6, \text{ and } x \text{ is not a multiple of } 15\}\\
A^c \cup B &= \{x \in \mathbb{N} \colon x \text{ is not a multiple of } 6, \text{ or } x \text{ is a multiple of } 15\}\\
A \cup B^c &= \{x \in \mathbb{N} \colon x \text{ is a multiple of } 6, \text{ or } x \text{ is not a multiple of } 15\}
\end{aligned}
$$

1.3. **Problem 3.** Let $A = \{x \in \mathbb{N} \colon x \text{ is a multiple of } 6\}$, and let $B = \{x \in \mathbb{N} \colon x \text{ is a multiple of } 3\}$. Let $\mathbb{N} = X$ be the universal set. What are: A^c? $(A^c)^c$? B^c? $A \cup B$? $A \cap B$? $A^c \cup B^c$? $A^c \cap B^c$? $(A \cap B)^c$? $(A \cup B)^c$? $A^c \cup B$? $A \cup B^c$? $(A^c \cup B)^c$? $(A \cup B^c)^c$? $A^c \cap B$? $A \cap B^c$?

$$
\begin{aligned}
A^c &= \{x \in \mathbb{N} \colon x \text{ is not a multiple of } 6\}\\
(A^c)^c &= A = \{x \in \mathbb{N} \colon x \text{ is a multiple of } 6\}\\
B^c &= \{x \in \mathbb{N} \colon x \text{ is not a multiple of } 3\}\\
A \cup B &= \{x \in \mathbb{N} \colon x \text{ is a multiple of } 3\}\\
A \cap B &= \{x \in \mathbb{N} \colon x \text{ is a multiple of } 6\}\\
A^c \cup B^c &= (A \cap B)^c = \{x \in \mathbb{N} \colon x \text{ is not a multiple of } 6\}\\
A^c \cap B^c &= (A \cup B)^c = \{x \in \mathbb{N} \colon x \text{ is not a multiple of } 3\}\\
(A \cap B)^c &= A^c \cup B^c = \{x \in \mathbb{N} \colon x \text{ is not a multiple of } 6\}\\
(A \cup B)^c &= A^c \cap B^c = \{x \in \mathbb{N} \colon x \text{ is not a multiple of } 3\}\\
A^c \cup B &= \{x \in \mathbb{N}\}\\
A \cup B^c &= \{x \in \mathbb{N} \colon x \text{ is a multiple of } 6, \text{ or } x \text{ is not a multiple of } 3\}\\
(A^c \cup B)^c &= \{x \in \mathbb{N}\}^c = \emptyset\\
(A \cup B^c)^c &= A^c \cap B = \{x \in \mathbb{N} \colon x \text{ is not a multiple of } 6, \text{ and } x \text{ is a multiple of } 3\}\\
A^c \cap B &= (A \cup B^c)^c = \{x \in \mathbb{N} \colon x \text{ is not a multiple of } 6, \text{ and } x \text{ is a multiple of } 3\}\\
A \cap B^c &= (A^c \cup B)^c = \{x \in \mathbb{N}\}^c = \emptyset
\end{aligned}
$$

1.4. **Problem 4.** Let $A = \{x \in \mathbb{N} \colon x \text{ is a multiple of } 5\}$, and let $B = \{x \in \mathbb{N} \colon x \text{ is a multiple of } 3\}$. Let $\mathbb{N} = X$ be the universal set. What are: A^c? $(A^c)^c$? B^c? $A \cup B$? $A \cap B$? $A^c \cup B^c$? $A^c \cap B^c$? $(A \cap B)^c$? $(A \cup B)^c$? $A^c \cup B$? $A \cup B^c$?

$$
\begin{aligned}
A^c &= \{x \in \mathbb{N} \colon x \text{ is not a multiple of } 5\} \\
(A^c)^c &= A = \{x \in \mathbb{N} \colon x \text{ is a multiple of } 5\} \\
B^c &= \{x \in \mathbb{N} \colon x \text{ is not a multiple of } 3\} \\
A \cup B &= \{x \in \mathbb{N} \colon x \text{ is a multiple of } 5, \text{ or } x \text{ is a multiple of } 3\} \\
A \cap B &= \{x \in \mathbb{N} \colon x \text{ is a multiple of } 15\} \\
A^c \cup B^c &= (A \cap B)^c = \{x \in \mathbb{N} \colon x \text{ is not a multiple of } 15\} \\
A^c \cap B^c &= \{x \in \mathbb{N} \colon x \text{ is not a multiple of } 5, \text{ and } x \text{ is not a multiple of } 3\} \\
(A \cap B)^c &= A^c \cup B^c = \{x \in \mathbb{N} \colon x \text{ is not a multiple of } 15\} \\
(A \cup B)^c &= A^c \cap B^c = \{x \in \mathbb{N} \colon x \text{ is not a multiple of } 5, \text{ and } x \text{ is not a multiple of } 3\} \\
A^c \cup B &= \{x \in \mathbb{N} \colon x \text{ is not a multiple of } 5, \text{ or } x \text{ is a multiple of } 3\} \\
A \cup B^c &= \{x \in \mathbb{N} \colon x \text{ is a multiple of } 5, \text{ or } x \text{ is not a multiple of } 3\}
\end{aligned}
$$

1.5. **Problem 5.** Try to prove that: $(A \cap B)^c = A^c \cup B^c$. Share your thinking on how to approach this problem.

Let P and Q be statements. We begin with the following truth table

P	Q	$\sim P$	$\sim Q$	$P \wedge Q$	$P \vee Q$	$P \Rightarrow Q$	$P \Leftrightarrow Q$	$(\sim P) \vee (\sim Q)$	$\sim (P \wedge Q)$
T	T	F	F	T	T	T	T	F	F
T	F	F	T	F	T	F	F	T	T
F	T	T	F	F	T	T	F	T	T
F	F	T	T	F	F	T	T	T	T

Table 1. A Truth Table

One reads the table as follows. The first two entries on the left side of a row define whether or not P and Q are true. For example, in the fourth row from the top, P is made to be false, and Q is made to be true. Within this row, operations on P and Q are calculated. For example, in the fourth row from the top, we see that $P \wedge Q$ is false, assuming P is false and Q is true, and so on. We now begin the proof.

Proof. Let $x \in X$. For the set A, we have a dichotomy: either $x \in A$ or $x \notin A$. Similarly, for B, we have a dichotomy: either $x \in B$ or $x \notin B$. Since we have two sets and two possibilities, there are exactly $2^2 = 4$ mutually exclusive cases to consider for the location of x: (i) $x \in A$ and $x \in B$ (ii) $x \in A$ and $x \notin B$ (iii) $x \notin A$ and $x \in B$ (iv) $x \notin A$ and $x \notin B$. Let P be the event $x \in A$ and let Q be the event $x \in B$. We can then translate the four cases above into statements in P and Q: (i) $P \wedge Q$ (ii) $P \wedge (\sim Q)$ (iii) $(\sim P) \wedge Q$ (iv) $(\sim P) \wedge (\sim Q)$. Note that $x \in (A \cap B)^c$ if and only if $\sim (P \wedge Q)$ is true. Also, $x \in A^c \cup B^c$ if and only if $(\sim P) \vee (\sim Q)$ is true. We want to show that $x \in (A \cup B)^c$ if and only if $x \in A^c \cap B^c$. So, to prove this, it suffices to show that $(\sim (P \wedge Q))$ is true if and only if $(\sim P) \vee (\sim Q)$ is true.

The Problem will then be proven if: given any of the four mutually exclusive cases (i),(ii),(iii),(iv), we determine that the truth of $\sim (P \wedge Q)$ is equal to the truth of $(\sim P) \vee (\sim Q)$. Now, cases (i) through (iv) correspond exactly to the assumptions of the last four rows of Table 1. Moreover, in Table 1, the column of $\sim (P \wedge Q)$ is equal to the column of $(\sim P) \vee (\sim Q)$. We conclude that $(\sim (P \wedge Q))$ is true if and only if $(\sim P) \vee (\sim Q)$ is true. The Problem is therefore proven. □

1.6. **Problem 6.** Prove the following. If p and q are two odd numbers, then $(p+q) \cdot (p-q)$ is a multiple of 4.

Proof. Since p and q are odd, there exists integers n, m such that $p = 2n+1$ and $q = 2m+1$. Observe

$$\begin{aligned}(p+q)(p-q) &= (2n+1+2m+1)(2n+1-2m-1) \\ &= 2(n+m+1)2(n+m) = 4(n+m+1)(n+m)\end{aligned} \qquad (*)$$

Since n, m are integers, $(n+m+1)$ and $(n+m)$ are integers. In particular, if we let $k = (n+m+1)(n+m)$, then k is an integer. Substituting k into equation $(*)$, we have

$$(p+q)(p-q) = 4k$$

Therefore, $(p+q)(p-q)$ is a multiple of 4, as desired. □

1.7. **Problem 7.** Assume that we know for sure that: All Pelicans Eat Fish (i.e. this is a true statement).

(a) Which of the following statements follows from the above statement?
(b) Which of the following statements cannot be true, if the above statement is true? (For question (b), only consider premises that are true in (i) through (vi).)

(i) If a bird is a Pelican, then it eats fish.
(ii) If a creature eats fish, then it is a Pelican.
(iii) If a bird is not a Pelican, then it does not eat fish.
(iv) If a creature does not eat fish, then it is not a Pelican.
(v) If a bird is a Pelican, then it does not eat fish.
(vi) If a creature does not eat fish, then it is a Pelican.

Let c be a creature. Let $P(c)$ be the event "c is a Pelican," let $F(c)$ be the event "c eats fish," let $B(c)$ be the event "c is a bird." Let b be a bird. (In particular, b is a creature.) We know that the following is true: for all creatures c, if $P(c)$ then $F(c)$. We now translate (i) through (vi) into logical form:

(i) If $P(b)$ then $F(b)$
(ii) If $F(c)$ then $P(c)$.
(iii) If $\sim P(b)$ then $\sim F(b)$.
(iv) If $\sim F(c)$ then $\sim P(c)$
(v) If $P(b)$ then $\sim F(b)$.
(vi) If $\sim F(c)$ then $P(c)$

Since b is a creature, (i) is true since we are given that the following is true for all creatures c: if $P(c)$ then $F(c)$. Now, (ii) is the converse of: if $P(c)$ then $F(c)$. However, we only know for sure the forward implication: for all c, if $P(c)$ then $F(c)$. Therefore, we do not know whether or not statement (ii) is true. In particular (ii) may be true, since all creatures may be Pelicans. But (ii) may also be false, if there are creatures other than Pelicans. Similarly, (iii) may be true, for example, if all birds are Pelicans. But (iii) may be false, if there is a bird that eats fish, and this bird is not a Pelican. Now, for all creatures c, if $P(c)$ then $F(c)$ is true. So, the contrapositive must also be true: for all creatures c, if $\sim F(c)$ then $\sim P(c)$. That is, we know that (iv) is true. To summarize so far, we know that (i) and (iv) are true, but we cannot be certain about the truth of (ii) and (iii).

We now examine (v). Consider the implication: if $P(b)$ then $\sim F(b)$. We know that the following implication is true for all creatures c: if $P(c)$ then $F(c)$. In particular, by the definition of this implication, $(\sim P(c)) \vee F(c)$ is true for all c. The implication that we are considering is: if $P(b)$ then $\sim F(b)$. By the definition of this implication, we want to know the truth of: $(\sim P(b)) \vee (\sim F(b))$. Assume that $P(b)$ is true. Then $\sim P(b)$ is false. Since b is a creature, we know that $(\sim P(b)) \vee F(b)$ is true. Therefore, $F(b)$ must be true. Since $\sim P(b)$ is false and $\sim F(b)$ is false, $(\sim P(b)) \vee (\sim F(b))$ is false. Therefore, the implication (if $P(b)$ then $\sim F(b)$) is false, given that $P(b)$ is true.

We now examine (vi). Consider the implication: if $\sim F(c)$ then $P(c)$. We know that the following implication is true for all creatures c: if $P(c)$ then $F(c)$. In particular, by the definition of this implication, $(\sim P(c)) \vee F(c)$ is true for all c. The implication that we are considering is: if $\sim F(c)$ then $P(c)$. By the definition of this implication, we want to know the truth of: $(F(c)) \vee (P(c))$. Assume that $\sim F(c)$ is true. Then $F(c)$ is false. Since $(\sim P(c)) \vee F(c)$ is true, we conclude that $\sim P(c)$ is true. Therefore, $P(c)$ is false. Since $F(c)$ is false and $P(c)$ is false, $(F(c)) \vee (P(c))$ is false. Therefore, the implication (if $\sim F(c)$ then $P(c)$) is false, given that $\sim F(c)$ is true.

We summarize our answer to the question below.

(a): (i) and (iv).

(b): (v) and (vi).

1.8. **Problem 8.** Assume that we know for sure that: In a faraway country named Shesing, all women that live there can sing (i.e. this is a true statement).

- (a) Which of the following statements follows from the above statement?
- (b) Which of the following statements cannot be true, if the above statement is true? (For question (b), only consider premises that are true in (i) through (vi).)

- (i) If you live in Shesing and are a woman, then you can sing.
- (ii) If you live in Shesing and can sing, then you are a woman.
- (iii) If you live in Shesing and are not a woman, then you cannot sing.
- (iv) If you live in Shesing and cannot sing, then you are not a woman.
- (v) If you live in Shesing and are a woman, then you cannot sing.
- (vi) If you live in Shesing and cannot sing, then you are a woman.

Let p be a person that lives in Shesing. Let $W(p)$ be the event "p is a woman," and let $S(p)$ be the event "p can sing." We know that the following is true: for all people p that are in Shesing, if $W(p)$ then $S(p)$. We now translate (i) through (vi) into logical form:

- (i) If $W(p)$ then $S(p)$
- (ii) If $S(p)$ then $W(p)$.
- (iii) If $\sim W(p)$ then $\sim S(p)$.
- (iv) If $\sim S(p)$ then $\sim W(p)$
- (v) If $W(p)$ then $\sim S(p)$.
- (vi) If $\sim S(p)$ then $W(p)$

Viewing the logical form of this Problem, we see that this question is essentially identical to Problem 7, with a few minor modifications. In particular, an identical analysis applies to (ii), (iv) and (vi) of this question. We therefore only discuss (i), (iii) and (v).

Let p be a person that lives in Shesing. Since p is a person that lives in Shesing, (i) is true. That is, (i) is just a repetition of the statement that we assume to be true in this problem. Now, (iii) is the contrapositive of (ii). Therefore, (iii) and (ii) must have the same truth value (for a fixed p). From our observation above of the similarity of this problem to the previous problem, we cannot be sure about the truth of (ii). Therefore, we cannot be sure about the truth of (iii).

We finally examine (v). Consider the implication: if $W(p)$ then $\sim S(p)$. We know that the following implication is true for all people p in Shesing: if $W(p)$ then $S(p)$. In particular, by the definition of this implication, $(\sim W(p)) \vee S(p)$ is true for all such p. The implication that we are considering is: if $W(p)$ then $\sim S(p)$. By the definition of this implication, we want to know the truth of: $(\sim W(p)) \vee (\sim S(p))$. Assume that $W(p)$ is true. Then $\sim W(p)$ is false. Since $(\sim W(p)) \vee S(p)$ is true, we conclude that $S(p)$ must be true. Since $\sim W(p)$ is false and $\sim S(p)$ is false, $(\sim W(p)) \vee (\sim S(p))$ is false. Therefore, the implication (if $W(p)$ then $\sim S(p)$) is false, given that $W(p)$ is true.

We summarize our answer to the question below.

(a): (i) and (iv).

(b): (v) and (vi).

1.9. **Problem 9.** For each of the following statements, determine whether it is always true, sometimes true, or never true:

(i) When you add two rational numbers, you get the same result as when you multiple them.
(ii) $(a+b)^2 = a^2 + b^2$, when $a, b \in \mathbb{R}$

(i) Let x, y be rational numbers. We are asked to check whether or not the following holds: $(x + y) = xy$. This assertion is sometimes true, since $(2+2) = 2 \cdot 2$. However, this assertion is not always true, since $(1+0) \neq 1 \cdot 0$. So, the assertion is only sometimes true.

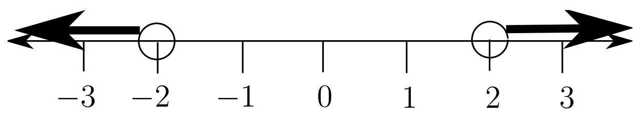
(ii) Let a, b be real numbers. Then $(a+b)^2 = a^2 + b^2$ is sometimes true, since $(0+1)^2 = 0^2 + 1^2$. However, this assertion is not always true, since $(1+1)^2 \neq 1^2 + 1^2$. So, the assertion is only sometimes true.

2. Homework 2

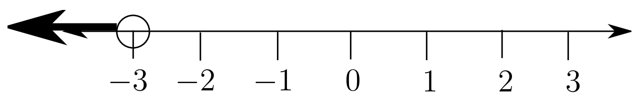
2.1. **Problem 1.** Let $A = \{x \in \mathbb{R} \colon x > 3 \text{ or } x < 2\}$, $B = \{x \in \mathbb{R} \colon x \leq 3 \text{ and } x > -1\}$, $C = \{x \in \mathbb{R} \colon x^2 > 4\}$, $D = \{x \in \mathbb{R} \colon x < 2 \text{ and } x^2 > 9\}$, and let $\mathbb{R} = X$ be the universal set.

(a) What are: A^c? $A \cup A^c$? B^c? $B \cup B^c$?
(b) What are: $A \cup B$? $A \cap B$?
(c) Describe C in a way that is easy to represent on a number line.
(d) Sketch a representation of C on a number line.
(e) What is C^c?
(f) Describe D in a way that is easy to represent on a number line.
(g) Sketch a representation of D on a number line
(h) What are: $A \cap D$? $A \cup D$?

(a) $A^c = \{x \in \mathbb{R} \colon 2 \leq x \leq 3\}$, $A \cup A^c = \mathbb{R}$, $B^c = \{x \in \mathbb{R} \colon x \leq -1 \text{ or } x > 3\}$, $B \cup B^c = \mathbb{R}$
(b) $A \cup B = \mathbb{R}$, $A \cap B = \{x \in \mathbb{R} \colon -1 < x < 2\}$
(c) $C = \{x \in \mathbb{R} \colon x < -2 \text{ or } x > 2\}$
(d)



(e) $C^c = \{x \in \mathbb{R} \colon -2 \leq x \leq 2\}$
(f) $D = \{x \in \mathbb{R} \colon x < -3\}$
(g)



(h) $A \cap D = D = \{x \in \mathbb{R} \colon x < -3\}$, $A \cup D = A = \{x \in \mathbb{R} \colon x > 3 \text{ or } x < 2\}$

2.2. **Problem 2.** For what values of x, $x \in \mathbb{R}$, is the following (open) statement true?

$$\frac{x^2 - 9}{x + 3} = x - 3$$

Explain your answer.

Note that $\frac{x^2-9}{x+3} = \frac{(x+3)(x-3)}{x+3}$. So, for $x \in \mathbb{R}$ with $x \neq -3$, we have $(x+3) \neq 0$, so we can perform a division as follows

$$\frac{x^2 - 9}{x + 3} = \frac{(x+3)(x-3)}{x+3} = (x - 3)$$

So, for $x \in \mathbb{R}$ with $x \neq -3$, the given open statement is true. For $x = -3$, $x + 3 = 0$, so $\frac{x^2-9}{x+3}$ is undefined. Therefore, the open statement is undefined for $x = -3$.

2.3. **Problem 3.** Is the following statement true? "For every $y, y \in \mathbb{R}$, there exists an $x, x \in \mathbb{R}$, such that $x^2 = y$." Explain your answer.

The statement is false. To see this, we will show that the negation of the statement is true. The negation of the statement is: "There exists $y, y \in \mathbb{R}$ such that, for all $x, x \in \mathbb{R}$, $x^2 \neq y$." Let $y = -1$ and let $x \in \mathbb{R}$. Since $x^2 \geq 0$ for all $x \in \mathbb{R}$, we conclude that $x^2 \neq -1$ for all $x \in \mathbb{R}$. Therefore, the negated statement is true, as claimed.

2.4. **Problem 4.** For what values of x and y, $x, y \in \mathbb{R}$, is the following (open) statement true? "$x^2 = y$." Explain your answer

Let $x, y \in \mathbb{R}$ with $x^2 = y$. Since $x^2 \geq 0$ for all $x \in \mathbb{R}$, the condition $x^2 = y$ can only be satisfied for $y \geq 0$. So, since $x^2 = y$, we may additionally assume that $y \geq 0$. In the case that $y \geq 0$, there exists x such that $x^2 = y$. In fact, if $y > 0$, there exist exactly two such $x \in \mathbb{R}$ such that $x^2 = y$. In the case $y = 0$, there exists only one x such that $x^2 = 0$. We define the following disjoint subsets of $\mathbb{R} \times \mathbb{R}$

$$D_+ = \{(x, y) \in \mathbb{R} \times \mathbb{R} \colon y > 0, x > 0, x^2 = y\},\ D_- = \{(x, y) \in \mathbb{R} \times \mathbb{R} \colon y > 0, x < 0, x^2 = y\}$$

We have shown: if the open statement is true, then $(x, y) \in D_+ \cup D_- \cup \{(0, 0)\}$. Now, assume that $(x, y) \in D_+ \cup D_- \cup \{(0, 0)\}$. For such $(x, y) \in \mathbb{R} \times \mathbb{R}$, the definitions of D_+ and D_- show immediately that (x, y) satisfies the open statement. Similarly, $(x, y) = (0, 0)$ satisfies the open statement. We therefore conclude: the open statement is true if and only if $(x, y) \in D_+ \cup D_- \cup \{(0, 0)\}$.

2.5. **Problem 5.** Examine the following (open) statement: "If n is an even number, then $(n^2 - 3n + 1)$ is positive."

(a) Give an example that contradicts the statement.
(b) Give an example that does not contradict the statement.
(c) Is the given (open) statement true? Explain your answer.
(d) What is the negation of this (open) statement?
(e) Is the negation true? Explain your answer.

(a) Let $n = 2$. Then n satisfies the premise of the open statement, but $n^2 - 3n + 1 = -1 \leq 0$, i.e. the conclusion of the statement is false. So, $n = 2$ contradicts the open statement.
(b) Let $n = 4$. Then n satisfies the premise of the open statement, and $n^2 - 3n + 1 = 5 > 0$, i.e. the conclusion of the statement is true. So $n = 4$ does not contradict the open statement.
(c) From (a) and (b), we have seen that the open statement is true for some even n, and not true for some other even n. So, the open statement can be true or false, depending on the value of n that is chosen.
(d) "n is an even number and $(n^2 - 3n + 1) \leq 0$ "
(e) From (a) and (b), we have seen that the negated open statement is true for some even n, and not true for some other even n. So, the negated open statement can be true or false, depending on the value of n that is chosen.

2.6. **Problem 6.** Examine the following (open) statement $(x, y \in \mathbb{R})$: "If $x < 2$ then $y > -3$."

(a) What would be a counterexample to this statement?
(b) What is the contrapositive of this statement?
(c) What is the negation of this statement?
(d) Is the negation true? Explain your answer.

(a) Let $(x, y) = (0, -4)$. Then $x < 2$, but $y \leq -3$. That is, the premise of the statement is true, but the conclusion of the statement is false. Therefore, $(x, y) = (0, -4)$ is a counterexample to the statement.
(b) "If $y \leq -3$ then $x \geq 2$"
(c) "$x < 2$ and $y \leq -3$"
(d) The negation is true for $(x, y) = (0, -4)$, but the negation is false for $(x, y) = (0, 0)$. So, the negation may be true or false, depending on the chosen values of x, y.

2.7. **Problem 7.** Examine the following (open) statement ($x \in \mathbb{R}$): "If $x^2 + 1 < 0$ then $-x^2 - 3 < 0$."
(a) Is the premise true?
(b) Is the conclusion true?
(c) Is the (open) statement true? Explain your answer.

(a) No, the premise is false. Let $x \in \mathbb{R}$. Then $x^2 \geq 0$, so $x^2 + 1 \geq 1 > 0$. So, for all $x \in \mathbb{R}$, $x^2 + 1 \geq 0$. Negating this statement (to get a false statement): there exists $x \in \mathbb{R}$ such that $x^2 + 1 < 0$. Since the latter statement is false, the premise ($x \in \mathbb{R}$) "If $x^2 + 1 < 0$" is always false.
(b) Yes, the conclusion is true. Let $x \in \mathbb{R}$. Then $x^2 \geq 0$, so $-x^2 \leq 0$, so $-x^2 - 3 < 0$. So, for all $x \in \mathbb{R}$, $-x^2 - 3 < 0$. Since the latter statement is true, the conclusion ($x \in \mathbb{R}$) "$-x^2 - 3 < 0$" is always true.
(c) Yes, the open statement is true for all $x \in \mathbb{R}$. Given any $x \in \mathbb{R}$, we showed in (a) and (b) that the premise of the statement is false, and the conclusion of the statement is true. For $x \in \mathbb{R}$, let $P(x)$ be the statement "$x^2 + 1 < 0$", and let $Q(x)$ be the statement "$-x^2 - 3 < 0$." We have shown in (a) and (b) that, for all $x \in \mathbb{R}$, $P(x)$ is false and $Q(x)$ is true. Since "If $P(x)$ then $Q(x)$" is defined as $(\sim P(x)) \vee Q(x)$, we conclude that "If $P(x)$ then $Q(x)$" is true, for all $x \in \mathbb{R}$.

2.8. **Problem 8.** Examine the following (open) statement ($x \in \mathbb{R}$): "If $x^2 + 1 < 0$ then $-x^2 - 3 > 0$."
(a) Is the premise true?
(b) Is the conclusion true?
(c) Is the (open) statement true? Explain your answer.

(a) No, the premise is false. Let $x \in \mathbb{R}$. Then $x^2 \geq 0$, so $x^2 + 1 \geq 1 > 0$. So, for all $x \in \mathbb{R}$, $x^2 + 1 \geq 0$. Negating this statement (to get a false statement): there exists $x \in \mathbb{R}$ such that $x^2 + 1 < 0$. Since the latter statement is false, the premise ($x \in \mathbb{R}$) "If $x^2 + 1 < 0$" is always false.
(b) No, the conclusion is false. Let $x \in \mathbb{R}$. Then $x^2 \geq 0$, so $-x^2 \leq 0$. So, for all $x \in \mathbb{R}$, $-x^2 - 3 \leq 0$. Negating this statement (to get a false statement): there exists $x \in \mathbb{R}$ such that $-x^2 - 3 > 0$. Since the latter statement is false, the conclusion ($x \in \mathbb{R}$) "$-x^2 - 3 > 0$" is always false.
(c) Yes, the open statement is true for all $x \in \mathbb{R}$. Given any $x \in \mathbb{R}$, we showed in (a) and (b) that the premise of the statement is false, and the conclusion of the statement is false. For $x \in \mathbb{R}$, let $P(x)$ be the statement "$x^2 + 1 < 0$", and let $Q(x)$ be the

statement "$-x^2 - 3 > 0$." We have shown in (a) and (b) that, for all $x \in \mathbb{R}$, $P(x)$ is false and $Q(x)$ is false. Therefore, $\sim P(x)$ is true for all $x \in \mathbb{R}$. Since "If $P(x)$ then $Q(x)$" is defined as $(\sim P(x)) \vee Q(x)$, we conclude that "If $P(x)$ then $Q(x)$" is true, for all $x \in \mathbb{R}$.

3. Homework 3

3.1. **Problem 1.** In class, we proved, without using a diagram, that for any two sets A and B: $(A \cap B)^c = A^c \cup B^c$. Use a similar method to prove that, for any two sets A and B: $(A \cup B)^c = A^c \cap B^c$.

Let P and Q be statements. We begin with the following truth table

P	Q	$\sim P$	$\sim Q$	$P \wedge Q$	$P \vee Q$	$P \Rightarrow Q$	$P \Leftrightarrow Q$	$(\sim P) \wedge (\sim Q)$	$\sim (P \vee Q)$
T	T	F	F	T	T	T	T	F	F
T	F	F	T	F	T	F	F	F	F
F	T	T	F	F	T	T	F	F	F
F	F	T	T	F	F	T	T	T	T

Table 2. A Truth Table

One reads the table as follows. The first two entries on the left side of a row define whether or not P and Q are true. For example, in the fourth row from the top, P is made to be false, and Q is made to be true. Within this row, operations on P and Q are calculated. For example, in the fourth row from the top, we see that $P \wedge Q$ is false, assuming P is false and Q is true, and so on. We now begin the proof.

Proof. Let $x \in X$. For the set A, we have a dichotomy: either $x \in A$ or $x \notin A$. Similarly, for B, we have a dichotomy: either $x \in B$ or $x \notin B$. Since we have two sets and two possibilities, there are exactly $2^2 = 4$ mutually exclusive cases to consider for the location of x: (i) $x \in A$ and $x \in B$ (ii) $x \in A$ and $x \notin B$ (iii) $x \notin A$ and $x \in B$ (iv) $x \notin A$ and $x \notin B$. Let P be the event $x \in A$ and let Q be the event $x \in B$. We can then translate the four cases above into statements in P and Q: (i) $P \wedge Q$ (ii) $P \wedge (\sim Q)$ (iii) $(\sim P) \wedge Q$ (iv) $(\sim P) \wedge (\sim Q)$. Note that $x \in (A \cup B)^c$ if and only if $\sim (P \vee Q)$ is true. Also, $x \in A^c \cap B^c$ if and only if $(\sim P) \wedge (\sim Q)$ is true. We want to show that $x \in (A \cup B)^c$ if and only if $x \in A^c \cap B^c$. So, to prove this, it suffices to show that $(\sim (P \vee Q))$ is true if and only if $(\sim P) \wedge (\sim Q)$ is true.

The Problem will then be proven if: given any of the four mutually exclusive cases (i),(ii),(iii),(iv), we determine that the truth of $\sim (P \vee Q)$ is equal to the truth of $(\sim P) \wedge (\sim Q)$. Now, cases (i) through (iv) correspond exactly to the assumptions of the last four rows of Table 2. Moreover, in Table 2, the column of $\sim (P \vee Q)$ is equal to the column of $(\sim P) \wedge (\sim Q)$. We conclude that $(\sim (P \vee Q))$ is true if and only if $(\sim P) \wedge (\sim Q)$ is true. The Problem is therefore proven. $\square$

3.2. **Problem 2.** Prove that, for any x that is an integer, if $(x^2 - 1)$ is not divisible by 3, then x is divisible by 3. Hint: It is easier to prove the contrapositive.

As suggested, we will prove the contrapositive of the statement. Since a statement is logically equivalent to its contrapositive, proving the contrapositive completes the Problem. The contrapositive is given by:

"For any $x \in \mathbb{Z}$, if x is not divisible by 3 then $(x^2 - 1)$ is divisible by 3." $(*)$

Let $x \in \mathbb{Z}$ such that x is not divisible by 3. Then there exists $k \in \mathbb{Z}$ such that either one of the following is satisfied. Case 1: $x = 3k + 1$, or, Case 2: $x = 3k + 2$. We consider each case separately.

Case 1. Let $x, k \in \mathbb{Z}$ with $x = 3k + 1$. We will prove that $(x^2 - 1)$ is divisible by 3. Observe

$$(x^2 - 1) = ((3k + 1)^2 - 1) = 9k^2 + 6k + 1 - 1 = 9k^2 + 6k = 3(3k^2 + 2k)$$

Since $k \in \mathbb{Z}$ we conclude that $3k^2 + 2k \in \mathbb{Z}$. So, letting $j = 3k^2 + 2k \in \mathbb{Z}$, we have shown that $x^2 - 1 = 3j$. Therefore, $x^2 - 1$ is divisible by 3.

Case 2. Let $x, k \in \mathbb{Z}$ with $x = 3k + 2$. We will prove that $(x^2 - 1)$ is divisible by 3. Observe

$$(x^2 - 1) = ((3k + 2)^2 - 1) = 9k^2 + 12k + 4 - 1 = 9k^2 + 12k + 3 = 3(3k^2 + 4k + 1)$$

Since $k \in \mathbb{Z}$ we conclude that $3k^2 + 4k + 1 \in \mathbb{Z}$. So, letting $j = 3k^2 + 4k + 1 \in \mathbb{Z}$, we have shown that $x^2 - 1 = 3j$. Therefore, $x^2 - 1$ is divisible by 3.

Since we have exhausted all cases, we conclude that statement $(*)$ is true, as desired.

3.3. **Problem 3.** Prove that, for any rational number n, if $n^5 - 6n^4 + 27 < 0$, then $n \leq 10$.

As in the previous Problem, it suffices to prove the contrapositive:

"For any rational number n, if $n > 10$ then $n^5 - 6n^4 + 27 \geq 0$" $(*)$

Let n be a rational number with $n > 10$. Since $n > 10$, $n - 6 > 4$. Therefore,

$$n^5 - 6n^4 + 27 = n^4(n - 6) + 27 > 10^4(4) + 27 = 40027 > 0$$

Since statement $(*)$ is true, and $(*)$ is the contrapositive of our desired statement, the Problem is complete.

3.4. **Problem 4.** The "divisibility by 3 rule" says that: If the sum of the digits of an integer n is divisible by 3, then n is divisible by 3.

(a) Prove the "divisibility by 3 rule" for 4-digit integers.
(b) What is the converse of the "divisibility by 3 rule"?
(c) Prove or disprove the converse of the "divisibility by 3 rule" for 4 digit integers.

(a) Let n be a 4-digit integer. Suppose first that $n \geq 0$. Let a be the "ones" digit of n, let b be the "tens" digit of n, let c be the "hundreds" digit of n, and let d be the "thousands" digit of n. If $n < 0$, then let a be the "ones" digit of n (multiplied by -1), let b be the "tens" digit of n (multiplied by -1), let c be the "hundreds" digit of n (multiplied by -1), and let d be the "thousands" digit of n (multiplied by -1). By the definitions of a, b, c, d, observe that a, b, c, d are integers with $-9 \leq a, b, c, d \leq 9$, and

$$n = a + 10b + 100c + 1000d \qquad (*)$$

Now, assume that the sum of the digits of the integer n are divisible by 3. By our definitions of a, b, c, d: there exists an integer k such that

$$a + b + c + d = 3k \qquad (**)$$

Let j be the integer $3b + 33c + 333d$. Since $9b + 99c + 999d = 3(3b + 33c + 333d) = 3j$, we combine $(*)$ and $(**)$ to get

$$\begin{aligned} n &= a + 10b + 100c + 1000d = (a + b + c + d) + (9b + 99c + 999d) \\ &= (a + b + c + d) + 3(3b + 33c + 333d) = 3k + 3j = 3(k + j) \end{aligned}$$

Since k and j are integers, $k + j$ is an integer, and we conclude that n is a multiple of 3.

(b) "If n is an integer and n is divisible by 3, then the sum of the digits of n is divisible by 3."

(c) We prove the converse statement. Let n be a 4-digit integer. Define a, b, c, d as in part (a). By the definitions of a, b, c, d, observe that a, b, c, d are integers with $-9 \leq a, b, c, d \leq 9$, and

$$n = a + 10b + 100c + 1000d \qquad (*)$$

Now, assume that n is divisible by 3. Then there exists an integer k such that

$$n = 3k \qquad (**)$$

Let j be the integer $3b + 33c + 333d$. Since $9b + 99c + 999d = 3(3b + 33c + 333d) = 3j$, we combine $(*)$ and $(**)$ to get

$$(a + b + c + d) = (a + 10b + 100c + 1000d) - (9b + 99c + 999d) = 3k - 3j = 3(k - j)$$

Since k and j are integers, $k - j$ is an integer, and we conclude that $(a+b+c+d)$ is divisible by 3. Since the sum of the digits of n is either $(a+b+c+d)$ or $-(a+b+c+d)$, we conclude that the sum of the digits of n is divisible by 3.

3.5. **Problem 5.** Find a mathematical implication that is true, for which its converse is also true.

(a) Formulate the statement as "if ..., then ..."
(b) Prove that it is true.
(c) Formulate its converse.
(d) Prove that the converse is true.

We use the following statement:

"If the sum of the digits of an integer n is divisible by 3, then n is divisible by 3."

In Problem 4, we proved this statement true, formulated its converse, and then proved the converse to be true.

3.6. **Problem 6.** Find a mathematical implication that is true, for which its converse is also false.

(a) Formulate the statement as "if ..., then ..."
(b) Prove that it is true.
(c) Formulate its converse.
(d) Prove that the converse is false.

(a) "For all $x \in \mathbb{R}$, if $x > 0$, then $x^2 > 0$"

(b) Let $x \in \mathbb{R}$. Suppose $x \leq 0$. Then the statement is automatically true, since the premise is not satisfied. Now, suppose $x > 0$. Then the premise is satisfied. Moreover, $x > 0$ implies $x^2 > 0$, so the conclusion is true. The statement "if $x > 0$, then $x^2 > 0$" has been proven for all $x \in \mathbb{R}$. Therefore, the statement from (a) is true.

(c) "For all $x \in \mathbb{R}$, if $x^2 > 0$, then $x > 0$"

(d) We will prove that the negation of the statement is true. The negation of the statement is: "There exists $x \in \mathbb{R}$ such that $x^2 > 0$ and $x \leq 0$." To prove the negation, let $x = -1$. Then $x^2 = 1 > 0$. Moreover, $-1 < 0$. Since we have found one such x, the negation of the statement from (c) is true. Therefore, the original statement from (c) is false.

3.7. **Problem 7.** Find another mathematical implication that is true, for which its converse is also false.

(a) Formulate the statement as "if ..., then ..."
(b) Prove that it is true.
(c) Formulate its converse.
(d) Prove that the converse is false.

(a) "For all $x, y \in \mathbb{R}$, if $xy > 0$ then $x^2 + y^2 > 0$"

(b) Let $x, y \in \mathbb{R}$. If $xy \leq 0$, then the premise is not satisfied, so the statement is true. If $xy > 0$, then we have two cases. Either (i) $x > 0$ and $y > 0$, or (ii) $x < 0$ and $y < 0$. In case (i), $x^2 > 0$ and $y^2 > 0$ so $x^2 + y^2 > 0$. In case (ii), $x^2 > 0$ and $y^2 > 0$, so $x^2 + y^2 > 0$. So, combining cases (i) and (ii): if $xy > 0$, then $x^2 + y^2 > 0$. We have proven the statement "if $xy > 0$ then $x^2 + y^2 > 0$" to be true for all $x, y \in \mathbb{R}$. Therefore, the statement from (a) is true.

(c) "For all $x, y \in \mathbb{R}$, if $x^2 + y^2 > 0$ then $xy > 0$"

(d) We will prove that the negation of the statement is true. The negation of the statement is: "There exists $x, y \in \mathbb{R}$ such that $x^2 + y^2 > 0$ and $xy \leq 0$." To prove the negation, let $(x, y) = (1, -1)$. Then $x^2 + y^2 = 2 > 0$. Moreover, $xy = -1 \leq 0$. Since we have found such a pair (x, y), the negation of the statement from (c) is true. Therefore, the original statement from (c) is false.

3.8. **Problem 8.** In class we discussed the following statement:

"If an integer n is a perfect square (i.e. n is the square of some integer), then n has an odd number of divisors" $\quad (*)$

Note that we include 1 and n as divisors of n. Also, note that the case $n = 0$ is excluded, since the divisors of 0 are not defined. Moreover, for both positive and negative n, we define a divisor of n to be positive.

(a) Prove that statement $(*)$ is indeed true.
(b) The number 10 has an even number of divisors, and 10 is not a perfect square. Explain how this finding is related to the contrapositive of statement $(*)$.
(c) It seems difficult to find an integer with an odd number of divisors that is not a perfect square. Can you formulate a conjecture using this observation?
(d) Formulate the converse of statement $(*)$.
(e) Is the converse of $(*)$ true?

Questions (a) and (e) are dealt with below. For (b), note that the contrapositive of $(*)$ is "If an integer n has an even number of divisors, then n is not a perfect square." So, the observation from (b) gives evidence for the contrapositive of $(*)$. For (c), we conjecture: "If a positive integer n has an odd number of divisors, then n is a perfect square." That is, we conjecture that the converse of $(*)$ is true, when restricted to positive integers. For (d), note that the actual converse of $(*)$ is "If an integer n has an odd number of divisors, then n is a perfect square."

For clarity, we give two proofs of Fact 1 below, which addresses (a) and (e). Strictly speaking, the converse of $(*)$ is false, since -4 has divisors $1, 2, 4$, but -4 is not a perfect square. However, if we restrict to positive integers, then the converse is actually true. To deduce $(*)$ from Fact 1 below, note that a nonzero perfect square is positive.

Fact 1: A positive integer n has an odd number of divisors if and only if n is a perfect square.

Proof. **(First proof of Fact 1)**: Let n be a positive integer. Let D be the set of divisors for n. Since $D \subseteq \{1, \ldots, n\}$, D is a finite set. Also, $1 \in D$, so D is nonempty. So, there exists a positive integer m such that D has m elements. Write $D = \{d_1, \ldots, d_m\}$, with $d_1 < d_2 < \cdots < d_m$, $d_1 = 1$, $d_m = n$.

Let $i \in \{1, \ldots, m\}$. Since d_i is a divisor of n, there exists a unique $j \in \{1, \ldots, m\}$ such that $d_i \cdot d_j = n$. (To see that d_j is uniquely determined by d_i, note that $d_j = n/d_i$, and all divisors d_j are distinct. So, if we are given d_i, d_j is determined by the formula $d_j = n/d_i$.) In particular, $d_1 d_m = n$. Now, if we begin with d_2, then there exists a unique $j \in \{1, \ldots, m\}$ such that $d_2 d_j = n$. Since $d_2 < d_3 < d_4 < \cdots < d_m$, d_j satisfies

$$d_j = n/d_2 > n/d_3 > n/d_4 > \cdots > n/d_m$$

Since $n/d_k \in D$ for $k = 3, 4, \ldots, m$, we conclude that d_j is larger than $m - 2$ elements of D. Now, $d_2 > d_1 = 1$, so $d_j = n/d_2 < n/d_1 = n = d_m$. So, d_j is smaller than one element of D. Combining these two facts about d_j, and using that D has exactly m elements, we conclude that d_j must be the second largest element of D. That is, $d_j = d_{m-1}$ and $d_2 d_{m-1} = n$.

We claim the following.

Claim 1. If $i, j \in \{1, \ldots, m\}$ satisfy $d_i d_j = n$, then $i + j = m + 1$.

We will prove this claim by induction on i. We proved the claim for $i = 1, 2$ above, and the inductive argument follows the same lines. By induction, assume that there exists $\ell \in \{1, \ldots, m-1\}$ such that Claim 1 holds for all $i, j \in \{1, \ldots, m\}$ with $i \leq \ell$. Let $i = \ell + 1$ and let d_j satisfy $d_i d_j = n$. To complete the induction, we must prove that, for $i = \ell + 1$, we must have $i + j = m + 1$. As above, $d_i < d_{i+1} < d_{i+2} < \cdots < d_m$, so

$$d_j = n/d_i > n/d_{i+1} > n/d_{i+2} > \cdots > n/d_m$$

Since $n/d_k \in D$ for $k = i+1, i+2, \ldots, m$, we conclude that d_j is larger than $m - i$ elements of D. Now, $d_i > d_{i-1} > \cdots > d_1 = 1$, so

$$d_j = n/d_i < n/d_{i-1} < n/d_{i-2} < \cdots < n/d_1 = n$$

So, d_j is smaller than $i-1$ elements of D. Combining these two facts about d_j, and using that D has exactly m elements, we conclude that $d_j = d_{m-(i-1)} = d_{m-i+1}$. That is, $d_i d_{m-i+1} = n$, $j = m - i + 1$, and $i + j = m + 1$, as desired. Thus, we have completed the inductive step, and Claim 1 is proven.

We can finally prove Fact 1. Suppose m is odd, with m defined above. Let $i = (m+1)/2$. Note that i is a positive integer. Let $j \in \{1, \ldots, m\}$ satisfy $d_i d_j = n$. Then $i + j = m + 1$ from Claim 1, i.e. $j = (m+1)/2 = i$, so $d_i d_j = d_i^2 = d_j^2 = n$. Therefore n is a perfect square. The forward implication of Fact 1 is proven. We now prove the converse: If n is a perfect square, then n has an odd number of divisors. Assume that n is a perfect square. Then there exists an $i \in \{1, \ldots, n\}$ and a divisor $d_i \in D$ such that $d_i^2 = n$. By Claim 1, we must have $2i = m + 1$, i.e. $m = 2i - 1$. Therefore, m is odd, as desired. The proof of Fact 1 is complete. $\square$

Proof. **(Second proof of Fact 1)**: Let n be a positive integer, and let m be the number of divisors of n. From the Fundamental Theorem of Arithmetic, there exists a unique positive integer k, there exist unique primes $p_1 < \cdots < p_k$ and there exist unique positive integers $a_1, \ldots, a_k$ such that

$$n = p_1^{a_1} \cdot p_2^{a_2} \cdots p_k^{a_k}$$

For example, $360 = 2^3 \cdot 3^2 \cdot 5$. We now prove the following explicit formula for m.

$$m = (a_1 + 1)(a_2 + 1) \cdots (a_k + 1) \qquad (\ddagger)$$

For example, if $n = 360$, then $m = 4 \cdot 3 \cdot 2 = 24$. We prove formula ($\ddagger$) by induction on k. Suppose $k = 1$. Then $n = p_1^{a_1}$. Let $D = \{1, p_1, p_1^2, \ldots, p_1^{a_1}\}$. Since elements of D are distinct divisors of n, we know that $m \geq a_1 + 1$. Now, let d be any divisor of n. By the Fundamental Theorem of Arithmetic, $d = p_1^j$ for some integer j such that $1 \leq j \leq a_1$. Therefore, $d \in D$, i.e. $m \leq a_1 + 1$. Combining our two inequalities for m, we conclude that $m = a_1 + 1$. So, the case $k = 1$ of the induction is complete.

Now, invoking the inductive hypothesis, suppose there exists a positive integer K such that ($\ddagger$) holds whenever $k \leq K$. The proof by induction will be complete if we prove formula ($\ddagger$) in the case $k = K + 1$. So let $k = K + 1$. Consider the integer n' defined by

$$n' = p_1^{a_1} \cdot p_2^{a_2} \cdots p_K^{a_K}$$

By the inductive hypothesis, the number of divisors of n' is $(a_1 + 1)(a_2 + 1) \cdots (a_K + 1)$. Let D' be the set of divisors of n', and let $D = \{1, p_k, p_k^2, p_k^3, \ldots, p_k^{a_k}\}$. For a set Y, let $|Y|$ denote the number of distinct elements of Y. Let $x', y' \in D'$ and let $x, y \in D$. By the Fundamental Theorem of Arithmetic, $x' \cdot x = y' \cdot y$ if and only if: $x' = y'$ and $x = y$. So,

$$|\{x' \cdot x \colon x' \in D', x \in D\}| \geq |D' \times D| = |D'| \cdot |D|$$

Now, for $x' \in D'$ and $x \in D$, each $x' \cdot x$ is a divisor of n, so

$$m \geq |D'| \cdot |D| = (a_1 + 1)(a_2 + 1) \cdots (a_K + 1) \cdot (a_{K+1} + 1)$$

Finally, let d be any divisor of n. By the Fundamental Theorem of Arithmetic, $d = x' \cdot x$ for some $x' \in D', x \in D$. So, $m \leq |D'| \cdot |D|$. We therefore conclude that

$$m = (a_1 + 1)(a_2 + 1) \cdot \cdots (a_{K+1} + 1)$$

So, the inductive proof of formula ($\ddagger$) is complete.

We can now prove Fact 1 via ($\ddagger$). Suppose n is a positive integer with an odd number of divisors. Let m be the number of divisors of n. As above, write $n = p_1^{a_1} \cdot p_2^{a_2} \cdots p_k^{a_k}$. From ($\ddagger$), $m = (a_1 + 1)(a_2 + 1) \cdots (a_k + 1)$. Since m is odd, for all integers i with $1 \leq i \leq k$, the integer $(a_i + 1)$ is odd. That is, for all integers i with $1 \leq i \leq k$, the integer a_i is even. So, let b_i be a non-negative integer such that $a_i = 2b_i$. Let N be the integer $N = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$.

Then $N^2 = n$, so n is a perfect square. The forward implication of Fact 1 is proven, so we proceed with the converse.

Now, assume that n is a nonzero perfect square. Then n is positive. As above, write $n = p_1^{a_1} \cdot p_2^{a_2} \cdots p_k^{a_k}$. For all integers i with $1 \leq i \leq k$, a_i is even, so $(a_i + 1)$ is odd, so $(a_1 + 1)(a_2 + 1) \cdots (a_k + 1)$ is odd. Therefore, (‡) says that the number of divisors of n is odd, as desired. □

4. Homework 4

4.1. Problem 1. In class, we filled the following Truth Table

P	Q	$P \Rightarrow Q$	$\sim P$	$\sim Q$	$(\sim Q) \Rightarrow (\sim P)$
T	T	T	F	F	T
T	F	F	F	T	F
F	T	T	T	F	T
F	F	T	T	T	T

Table 3. A Truth Table

We saw that the implication $P \Rightarrow Q$ and its contrapositive $(\sim Q) \Rightarrow (\sim P)$ have the same Truth values. This fact can be used to prove that these two statements are equivalent.

(i) We fill the following Truth Table. Based on this Table, we find a statement that is equivalent to $P \Rightarrow Q$ and $(\sim Q) \Rightarrow (\sim P)$.

P	Q	$P \vee Q$	$(\sim P) \vee Q$	$P \vee (\sim Q)$
T	T	T	T	T
T	F	T	F	T
F	T	T	T	F
F	F	F	T	T

Table 4. A Truth Table

Note that the third column of Table 3 is equal to the fourth column of Table 4. Also, the final four rows of both of these Tables exhaust all possible combinations of values of P and Q. We therefore conclude that $P \Rightarrow Q$ is equivalent to $(\sim P) \vee Q$.

(ii) We fill the following Truth Table. Based on this Table, we find the negation of $P \vee (\sim Q)$

P	Q	$P \wedge Q$	$(\sim P) \wedge Q$	$P \wedge (\sim Q)$
T	T	T	F	F
T	F	F	F	T
F	T	F	T	F
F	F	F	F	F

Table 5. A Truth Table

Note that the fifth column of Table 4 is the negation of the fourth column of Table 5. Also, the final four rows of both of these Tables exhaust all possible combinations of values of P and Q. We therefore conclude that $(\sim P) \wedge Q$ is the negation of $P \vee (\sim Q)$.

(iii) We fill the following Truth Table. Based on this Table, we will mention some connections to the above Truth Tables.

P	Q	$P \Rightarrow Q$	$Q \Rightarrow P$	$P \Leftrightarrow Q$
T	T	T	T	T
T	F	F	T	F
F	T	T	F	F
F	F	T	T	T

Table 6. A Truth Table

The third column of Table 6 is the negation of the fifth column of Table 5. The fourth column of Table 6 is equal to the fifth column of Table 4, and the fourth column of Table 6 is equal to the negation of the fourth column of Table 5. As noted before, the final four rows of these Tables exhaust all possible combinations of values of P and Q. We therefore conclude: $P \Rightarrow Q$ is the negation of $P \wedge (\sim Q)$, $Q \Rightarrow P$ is equivalent to $P \vee (\sim Q)$, and $Q \Rightarrow P$ is the negation of $(\sim P) \wedge Q$.

4.2. **Problem 2.** In class we investigated properties of 3-digit numbers that are divisible by 37, and we presented at least two ideas for proving a proposed conjecture.

(i) Write a full and well constructed proof of the following claim: If a 3-digit integer n is divisible by 37, then any 3-digit integer that is obtained by a cyclic change of the digits of n is also divisible by 37.

(ii) Does your proof work for 4-digit numbers? Explain your answer.

Proof. (of (i)) Let n be a 3 digit integer that is divisible by 37. Since we will prove a statement about cyclic permutations of the digits of n, it suffices to consider the absolute value of n. That is, we may assume that n is a non-negative integer. Let a be the "hundreds" digit of n, let b be the "tens" digit of n, and let c be the "ones" digit of n. Thus, a, b, c are integers and $0 \leq a, b, c \leq 9$. Moreover, $n = 100a + 10b + c$. Consider the cyclic permutation m of n such that $m = 100b + 10c + a$. By our assumption on n, there exists an integer k such that $n = 37k$. Now, observe

$$\begin{aligned} 10n &= 10(100a + 10b + c) = 1000a + 100b + 10c \\ &= (100b + 10c + a) + 999a = m + 999a = m + 37 \cdot (27a) \end{aligned}$$

So, $m = 10n - 37 \cdot (27a) = 37(10k - 27a)$. Since a and k are integers, $10k - 27a$ is an integer. Let $A = 10k - 27a$. Combining the previous sentences, $m = 37A$, i.e. m is a multiple of 37.

Now, consider the cyclic permutation r of n such that $r = 100c + 10a + b$. By the result that we must proved, there exists an integer ℓ such that $m = 37\ell$. Now, observe

$$\begin{aligned} 10m &= 10(100b + 10c + a) = 1000b + 100c + 10a \\ &= (100c + 10a + b) + 999b = r + 999b = r + 37 \cdot (27b) \end{aligned}$$

So, $r = 10m - 37 \cdot (27b) = 37(10\ell - 27b)$. Since ℓ and b are integers, $10\ell - 27b$ is an integer. Let $B = 10\ell - 27b$. Combining the previous sentences, $r = 37B$, i.e. r is a multiple of 37.

Finally, since m and r are the only two nontrivial cyclic permutations of n, the proof is complete. $\square$

(ii) The same trick that allows (i) to work does not seem to work for four digit integers. Specifically, for the same trick to work, we would need 9999 to be a multiple of 37. However, 9999 is not a multiple of 37. Indeed, if we try to extend the claim from (i) to four digit integers, we will be unsuccessful. For a counterexample to such a claim, consider $n = 3700$. Since $n = 37 \cdot 100$, n is a multiple of 37. However, $m = 7003$ is a cyclic permutation of n, and m is not a multiple of 37.

4.3. **Problem 3.** Let a and b be positive real numbers such that $b > a > 0$. Prove the following.

(i) $a < (a+b)/2 < b$
(ii) $a < \sqrt{a \cdot b} < b$
(iii) $(a+b)/2$ is the arithmetic mean of a and b, and $\sqrt{a \cdot b}$ is the geometric mean of a and b. Write in your own words what you proved in (i) and (ii) about these means.

Proof. (of (i)) We will prove each inequality separately. We first prove that $a < (a+b)/2$. Since $b > a > 0$, we see that $b/2 > a/2$. So, $(a+b)/2 = (a/2) + (b/2) > (a/2) + (a/2) = a$. We now prove that $(a+b)/2 < b$. Once again, since $b > a > 0$, we see that $a/2 < b/2$. So, $(a+b)/2 = (a/2) + (b/2) < (b/2) + (b/2) = b$. Since both inequalities are proven, we are done. $\square$

Proof. (of (ii)) We will prove each inequality separately. We first prove that $a < \sqrt{a \cdot b}$. Since $b > a > 0$, we get $\sqrt{b} > \sqrt{a} > 0$. So, $\sqrt{a \cdot b} = \sqrt{a} \cdot \sqrt{b} > \sqrt{a} \cdot \sqrt{a} = a$. We now prove that $\sqrt{a \cdot b} < b$. Once again, since $b > a > 0$, we get $0 < \sqrt{a} < \sqrt{b}$. So, $\sqrt{a \cdot b} = \sqrt{a} \cdot \sqrt{b} < \sqrt{b} \cdot \sqrt{b} = b$. Since both inequalities are proven, we are done. $\square$

(iii) Let a and b be positive integers. We have shown that the arithmetic mean and geometric mean lie in between a and b (with respect to their positions on the real line).

4.4. **Problem 4.** Provide a definition and some examples for each of the following:

(a) A prime number
(b) A rational number
(c) An irrational number

(a) Let p be a positive integer such that $p > 1$. We say that p is a prime number if and only if the following is satisfied: if we write $p = ab$ with a, b positive integers, then either a or b is equal to 1. The first few prime numbers are $2, 3, 5, 7, 11, 13, \ldots$.

(b) Let p, q be integers with $q \neq 0$. A rational number n is any number of the form $n = p/q$. Some examples include $4, 2, 1/2, 25/34, \ldots$.

(c) Let n be a real number. We say that n is irrational if and only if n is not rational. So, n is irrational if and only if: n cannot be expressed as a ratio p/q of two integers p and q. It is not so easy to come up with examples of irrational numbers, but we will show: if P is a prime, then $\sqrt{P}$ is irrational. In particular, $\sqrt{2}$ and $\sqrt{3}$ are irrational.

Proof. Let P be a prime number. We show that $\sqrt{P}$ is irrational. We argue by contradiction. Suppose $\sqrt{P}$ is rational. Let p', q' be integers with $q' \neq 0$ such that $\sqrt{P} = p'/q'$. Since $\sqrt{P} > 0$, we may assume that $p', q' > 0$. Let D be the greatest common divisor of p' and q'. That is, D is the largest integer such that: there exist positive integers p, q such that $p' = Dp$ and $q' = Dq$. Given D, let p, q be positive integers such that $p' = Dp$ and $q' = Dq$. Note that $q \neq 0$ since $q' \neq 0$ and $D \geq 1$. Now,

$$\sqrt{P} = \frac{p'}{q'} = \frac{Dp}{Dq} = \frac{p}{q} \qquad (*)$$

The fraction p/q is known as the fraction in "least terms." By the definition of D, the following two sets are disjoint: the set of prime divisors of p and the set of prime divisors of q. However, $(*)$ says that $P = p^2/q^2$, i.e. $p^2 = Pq^2$. So, since p and q are positive integers and P is a prime number, the Fundamental Theorem of Arithmetic implies that P is a divisor of p. So, there exists a positive integer M such that $p = PM$. Then, $Pq^2 = p^2 = P^2M^2$, i.e. $q^2 = PM^2$ (using $P \neq 0$, which follows since P is prime). So, since q and M are positive integers and P is a prime number, the Fundamental Theorem of Arithmetic implies that P is a divisor of q.

In summary, p and q both have P as a divisor. However, we deduced above that p and q do not share any prime factors. We have arrived at a contradiction. We therefore conclude that $\sqrt{P}$ is irrational for P prime. □

4.5. **Problem 5.**

(i) Is 1 a prime number? Explain.
(ii) Is a product of two prime numbers a prime number? Explain.

(i) 1 is not a prime number. In our definition of a prime number, we required a prime number to be an integer greater than 1.

(ii) The product of two prime numbers is not a prime number. To see this, let p and q be prime numbers, and let $n = pq$. Since p and q are prime numbers, p and q are positive integers that are greater than 1. In particular, n is a positive integer greater than 1. However, we can write $n = pq$ with p, q positive integers that are greater than 1. That is, the definition of a prime number is not satisfied.

5. Homework 5

5.1. **Problem 1.** In class we proved the triangle inequality. That is, for any real numbers a, b the following inequality holds: $|a + b| \leq |a| + |b|$. Prove that for any real numbers a, b the following inequality holds: $|a| - |b| \leq |a + b|$.

Proof. Let a, b be real numbers. Let $c = a + b$ and let $d = -b$. From the triangle inequality, $|c + d| \leq |c| + |d|$. So, substituting in the definitions of c and d, we get $|a| \leq |a + b| + |b|$, i.e. $|a| - |b| \leq |a + b|$. □

5.2. **Problem 2.** Let a, b be real numbers such that $0 < a < b$. Which mean is larger: the arithmetic mean, $(a+b)/2$, or the geometric mean, $\sqrt{a \cdot b}$?

Proof. Let a, b be real numbers such that $0 < a < b$. We show that the geometric mean is less than the arithmetic mean. Since $0 < a < b$, $0 < \sqrt{a} < \sqrt{b}$, so $\sqrt{b} - \sqrt{a} > 0$, and $(\sqrt{b} - \sqrt{a})^2 > 0$. Therefore, $b + a - 2\sqrt{ab} > 0$, i.e. $(b+a)/2 > \sqrt{ab}$, as desired. $\square$

5.3. **Problem 3.** Let a, b be real numbers such that $0 < a < b$. The harmonic mean of a and b is defined as $1/\left(\frac{1}{2}\left(\frac{1}{a} + \frac{1}{b}\right)\right)$. (By multiplying the numerator and denominator by $a \cdot b \neq 0$, we can rewrite the harmonic mean as $2ab/(a+b)$). The root mean square of a and b is defined as $\sqrt{(a^2+b^2)/2}$. The contraharmonic mean of a and b is defined as $(b^2+a^2)/(b+a)$. Find an ordering for these means.

Proof. Let a, b be real numbers such that $0 < a < b$. We prove the following four inequalities.

$$\frac{2ab}{a+b} < \sqrt{ab} < \frac{a+b}{2} < \sqrt{\frac{a^2+b^2}{2}} < \frac{b^2+a^2}{b+a} \qquad (*)$$

We begin with the inequality on the left, and we will prove each of the four inequalities by successively moving one step to the right in $(*)$.

Since $0 < a < b$, $0 < a^2 < b^2$. Applying the result of Problem 2 to a^2 and b^2, we get $ab < (a^2+b^2)/2$, so $2ab < a^2+b^2$. Multiplying both sides by $a \cdot b$ and noting that $a \cdot b > 0$, we get $2a^2b^2 < a^3b + b^3a$. Adding $2a^2b^2$ to both sides gives $4a^2b^2 < a^3b + b^3a + 2a^2b^2$. Factoring out $a \cdot b$ on the right side, we get $4a^2b^2 < ab(a^2+b^2+2ab) = ab(a+b)^2$. Since $a, b > 0$, $(a+b)^2 > 0$ so we can divide by $(a+b)^2$ to get $4a^2b^2/(a+b)^2 < ab$. Since $a, b > 0$, $a \cdot b > 0$. Also $4a^2b^2/(a+b)^2 = (2ab/(a+b))^2 \geq 0$. So, we can take the square root of both sides of our inequality to deduce the first inequality of $(*)$:

$$\frac{2ab}{a+b} < \sqrt{ab}$$

The second inequality of $(*)$ is exactly the arithmetic mean geometric mean inequality, which we proved in Problem 2. We therefore begin to prove the third inequality of $(*)$. As in our proof of the first inequality of $(*)$, we have $ab < (a^2+b^2)/2$. Multiplying both sides by $1/2$, we get $ab/2 < (a^2+b^2)/4$. Adding $(a^2+b^2)/4$ to both sides, we have $(a^2+b^2+2ab)/4 = ((a+b)/2)^2 < (a^2+b^2)/2$. Since both sides of the inequality are positive, we may take the square root of both sides and conclude the third inequality of $(*)$:

$$\frac{a+b}{2} < \sqrt{\frac{a^2+b^2}{2}}$$

We now conclude the problem by proving the fourth inequality of $(*)$. As in our proof of the first inequality of $(*)$, we have $ab < (a^2+b^2)/2$. Multiply both sides of this inequality by 2 and then add a^2+b^2 to both sides of the result to get $a^2+b^2+2ab < 2b^2+2a^2$. That is, $(a+b)^2 < 2(a^2+b^2)$. Since $a^2+b^2 > 0$, we can multiply both sides of our inequality by a^2+b^2 to get $(a^2+b^2)(a+b)^2 < 2(a^2+b^2)^2$. Since $(a+b)^2 > 0$, we can divide both sides by $(a+b)^2$ to get $(a^2+b^2) < 2(a^2+b^2)^2/(a+b)^2$. Both sides of this inequality are positive, so we can divide both sides by 2 and then take the square root of both sides to conclude the final inequality of $(*)$:

$$\sqrt{\frac{a^2+b^2}{2}} < \frac{b^2+a^2}{b+a}$$

□

5.4. **Problem 4.** Let a, b, c, d be real numbers. Assume that the fractions a/b and c/d are positive, and $0 < a/b < c/d$ (in particular, $b \neq 0$ and $d \neq 0$). We want to know whether or not the following inequality is satisfied: $(a/b) < (a+c)/(b+d) < c/d$.

In general, the inequality is not satisfied. Let $a = 1, b = 3, c = -1, d = -2$. Then a/b and c/d are positive, and $0 < a/b < c/d$. However, $(a+c)/(b+d) = 0$, and $0 < a/b$, so the inequality that we want to prove cannot be satisfied. However, if we restrict to the case where $a, b, c, d > 0$, then the inequality is true.

Proof. Let a, b, c, d be real numbers such that $a, b, c, d > 0$. We will prove that $(a/b) < (a+c)/(b+d) < c/d$. Since $a/b < c/d$ and $b, d > 0$, we know that $ad < bc$, so $ad+ab < bc+ab$, i.e. $a(b+d) < b(a+c)$. Since $b+d$ and b are both positive, we can multiply both sides of our inequality by $1/(b(b+d))$ to get $a/b < (a+c)/(b+d)$. So, the first desired inequality holds. The second inequality follows similarly. As before, $ad < bc$, so $ad+cd < bc+cd$, i.e. $d(a+c) < c(b+d)$. Since $b+d$ and d are both positive, we can multiply both sides of our inequality by $1/(d(b+d))$ to get $(a+c)/(b+d) < c/d$. □

6. Homework 6

6.1. **Problem 1.** In the following problem, we fill in the details from a skeleton proof.

It is given that $n \in \mathbb{Z}$ and $5n - 7$ is even. We prove that n is odd.

Proof. Since $5n-7$ is even, there exists $k \in \mathbb{Z}$ such that $5n - 7 = 2k$. So, $5n = 2k+7$, that is, $5n$ is an even number plus an odd number, so $5n$ is odd. Given any $j \in \mathbb{Z}$, if $5j$ is odd, then the prime factorization of $5j$ does not contain 2. Therefore, the prime factorization of j does not contain 2, i.e. j is odd. In particular, setting $j = n$, we see that n is odd, as desired. □

6.2. **Problem 2.** In the following problem, we fill in the details from a skeleton proof.

It is given that x and y are integers of the same parity. We prove that $x^2 - y^2$ is divisible by 4.

Proof. Since x and y are of the same parity we have exactly two cases to consider. In case 1, there exist $m, \ell \in \mathbb{Z}$ such that $x = 2m$ and $y = 2\ell$. In case 2, there exists $m, \ell \in \mathbb{Z}$ such that $x = 2m+1$ and $y = 2\ell+1$. In either case, note that there exist $n, k \in \mathbb{Z}$ such that $x+y = 2n$ and $x - y = 2k$. Therefore, $(x^2 - y^2) = (x+y)(x-y) = 4nk$, i.e. $(x^2 - y^2)/4 = nk$. Since $n, k \in \mathbb{Z}$, $nk \in \mathbb{Z}$, i.e. $(x^2 - y^2)/4 \in \mathbb{Z}$, as desired. □

6.3. **Problem 3.** In the following problem, we fill in the details from a skeleton proof.

(a) It is given that $x, y \in \mathbb{R}$ are two positive numbers. We will show that their arithmetic mean is larger than or equal to their geometric mean.

Proof. Since $(x-y) \in \mathbb{R}$, $(x-y)^2 \geq 0$. So, $x^2+y^2-2xy \geq 0$. Adding $4xy$ to both sides gives $x^2+y^2+2xy \geq 4xy$, i.e. $(x+y)^2 \geq 4xy$. Since $x, y > 0$, $xy > 0$. Since $x+y \in \mathbb{R}$, $(x+y)^2 \geq 0$. So, we can take the square root of both sides of the inequality $(x+y)^2 \geq 4xy$ while preserving the inequality. So, $|x+y| \geq 2\sqrt{xy}$. Since $x, y > 0$, $x+y > 0$, so the inequality can be rewritten as $x+y \geq 2\sqrt{xy}$. Dividing both sides of this inequality by 2 gives $(x+y)/2 \geq \sqrt{xy}$, as desired. $\square$

(b) It is given that $x, y \in \mathbb{R}$ are two positive numbers and $\sqrt{xy} = (x+y)/2$. We will prove that $x = y$.

Proof. Multiplying both sides of the given equation by 2 gives $2\sqrt{xy} = x+y$. Squaring both sides of this equation gives $x^2+y^2+2xy = 4xy$, i.e. $x^2+y^2-2xy = 0$, i.e. $(x-y)^2 = 0$. Since both sides of this equation are zero, we can take the square root of both sides while preserving the equality. We conclude that $|x-y| = 0$, i.e. $x = y$, as desired. $\square$

6.4. **Problem 4.** We first give a full proof of a fact. We then present flawed proofs of the same fact. We point out the flaws, inaccuracies, and redundancies in the flawed proofs. Our extra comments are written in bold typeface.

Let $x, y \in \mathbb{R}$. We prove that $|xy| = |x|\,|y|$.

Proof. For a real number r, define the absolute value by

$$|r| = \begin{cases} r & \text{, if } r \geq 0 \\ -r & \text{, if } r \leq 0 \end{cases}$$

There are exactly three cases that we need to check. These cases cover all possible values of x and y.

Case 1: $x \geq 0, y \geq 0$. Case 2: $x \geq 0, y \leq 0$. Case 3: $x \leq 0, y \leq 0$. Note that there is a fourth case where $x \leq 0$ and $y \geq 0$. However, assuming this case occurs, if we define $y' = x$ and $x' = y$ and then substitute x', y' into Case 2, we see that Case 3 subsumes the present case. Note also that any $x, y \in \mathbb{R}$ must be covered by these cases since x satisfies $x \geq 0$ or $x \leq 0$, and y satisfies $y \geq 0$ or $y \leq 0$. So, proving $|xy| = |x|\,|y|$ for each of these cases proves the desired assertion for all $x, y \in \mathbb{R}$.

We first consider Case 1. In this case $x \geq 0$, so $|x| = x$, and $y \geq 0$ so $|y| = y$ by the definition of absolute value. Together, these statements imply that $|x|\,|y| = xy$. Now, $x \geq 0$ and $y \geq 0$, so $xy \geq 0$. That is, by the definition of absolute value, $|xy| = xy$. Combining our two equalities, we get $|xy| = xy = |x|\,|y|$.

We now consider Case 2. In this case $x \geq 0$, so $|x| = x$, and $y \leq 0$ so $|y| = -y$ by the definition of absolute value. Together, these statements imply that $|x|\,|y| = x(-y) = -xy$. Now, $x \geq 0$ and $y \leq 0$, so $xy \leq 0$. That is, by the definition of absolute value, $|xy| = -xy$. Combining our two equalities, we get $|xy| = -xy = |x|\,|y|$.

We finally consider Case 3. In this case $x \le 0$, so $|x| = -x$, and $y \le 0$ so $|y| = -y$ by the definition of absolute value. Together, these statements imply that $|x|\,|y| = (-x)(-y) = xy$. Now, $x \le 0$ and $y \le 0$, so $xy \ge 0$. That is, by the definition of absolute value, $|xy| = xy$. Combining our two equalities, we get $|xy| = xy = |x|\,|y|$.

Since all cases have been exhausted, we are done. $\square$

Flawed Proof 1

[The given has not been stated. The statement that is to be proven has not been stated. An explanation of the different cases has not been given. The numbers b and a have not been defined properly. Presumably, $a, b \ge 0$.]

Case 1. Let $x = -a$ and let $y = -b$. Then $|(-a)(-b)| = |-a|\,|-b|$ and $ab = ab$. **[The assertion $ab = ab$ is superfluous, and the equation $|(-a)(-b)| = |-a|\,|-b|$ has not been explicitly justified. Moreover, the assertion $|xy| = |x|\,|y|$ has not been stated explicitly.]**

Case 2. Let $x = -a$ and let $y = b$. Then $|(-a)(b)| = |-a|\,|b|$ and $ab = ab$. **[The assertion $ab = ab$ is superfluous, and the equation $|(-a)(b)| = |-a|\,|b|$ has not been explicitly justified. Moreover, the assertion $|xy| = |x|\,|y|$ has not been stated explicitly.]**

Case 3. Let $x = a$ and let $y = b$. Then $|ab| = |a|\,|b|$ and $ab = ab$. **[The assertion $ab = ab$ is superfluous, and the equation $|ab| = |a|\,|b|$ has not been explicitly justified.]**

[Finally, no indication is given that the proof is complete.]

Flawed Proof 2

[The given has not been stated, and x and y have not been defined.]

We prove that $|xy| = |x|\,|y|$.

Proof. Assuming $|xy| = |x|\,|y|$, square both sides to get $(xy)^2 = x^2y^2$. **[In a proof, one should not assume the thing that is to be proven. One needs to show that the given information logically implies the conclusion. However, $(xy)^2 = x^2y^2$ is true, and we can just begin with this fact.]** Taking the square root of both sides gives $\sqrt{(xy)^2} = \sqrt{x^2y^2}$. Therefore $xy = \sqrt{x^2} \cdot \sqrt{y^2}$. **[Actually, we should conclude that $|xy| = \sqrt{x^2}\sqrt{y^2}$.]** Therefore $xy = xy$. **[Actually, we should conclude that $|xy| = |x|\,|y|$, which is what we set out to prove.]** $\square$

Flawed Proof 3

It is given that $x, y \in \mathbb{R}$. We will prove that $|xy| = |x|\,|y|$.

Proof. After multiplying x and y together, we get some quantity, and then taking absolute values of this quantity gives a positive number. Putting absolute values around x and y separately also gives positive numbers. The result $|x|\,|y|$ must result in the same value as $|xy|$. **[The assertion about the signs of the quantities is correct, but the final assertion has not been proven rigorously.] [Lastly, no mention of the end of the proof is given.]**

6.5. **Problem 5.** We first give a full proof of a fact. We then present flawed proofs of the same fact. We point out the flaws, inaccuracies, and redundancies in the flawed proofs. Our extra comments are written in bold typeface.

We prove assertion (a) and answer questions (b) through (e).

(a) For $n \in \mathbb{N}, n \geq 6$, we show that $n^3 - 3n^2 - 9 \geq 0$.
(b) For $n \in \mathbb{N}, n > 6$, is it true that $n^3 - 3n^2 - 9 \geq 0$?
(c) For $n \in \mathbb{N}, n \geq 10$, is it true that $n^3 - 3n^2 - 9 \geq 0$?
(d) For $n \in \mathbb{N}, n \geq 4$, is it true that $n^3 - 3n^2 - 9 \geq 0$?
(e) For $n \in \mathbb{N}, n \geq 2$, is it true that $n^3 - 3n^2 - 9 \geq 0$?

Proof. (of part (a)). Let $n \geq 6, n \in \mathbb{N}$. We show that $n^3 - 3n^2 - 9 \geq 0$. Since $n \geq 6$, we conclude that $n - 3 \geq 3$ and $n^2 \geq 36$. Therefore, $(n-3)n^2 - 9 \geq 3 \cdot 36 - 9 = 99 \geq 0$. Rewriting this inequality, we have $n^3 - 3n^2 - 9 \geq 0$, as desired. □

(b) Yes, $n^3 - 3n^2 - 9 \geq 0$ for $n > 6, n \in \mathbb{Z}$. We proved that $n^3 - 3n^2 - 9 \geq 0$ for all $n \geq 6, n \in \mathbb{Z}$. So, in particular, $n^3 - 3n^2 - 9 \geq 0$ for all $n > 6, n \in \mathbb{Z}$.

(c) Yes, $n^3 - 3n^2 - 9 \geq 0$ for $n \geq 10, n \in \mathbb{Z}$. We proved that $n^3 - 3n^2 - 9 \geq 0$ for all $n \geq 6, n \in \mathbb{Z}$. So, in particular, $n^3 - 3n^2 - 9 \geq 0$ for all $n \geq 10, n \in \mathbb{Z}$.

(d) Yes, $n^3 - 3n^2 - 9 \geq 0$ for $n \geq 4, n \in \mathbb{Z}$. We proved that $n^3 - 3n^2 - 9 \geq 0$ for all $n \geq 6, n \in \mathbb{Z}$, so to answer part (d) affirmatively, it suffices to show that $n^3 - 3n^2 - 9 \geq 0$ for $n = 4$ and $n = 5$. Finally, we can check explicitly that $(4)^3 - 3(4)^2 - 9 = 7 \geq 0$ and $(5)^3 - 3(5)^2 - 9 = 41 \geq 0$.

(e) No, the inequality $n^3 - 3n^2 - 9 \geq 0$ does not hold for all $n \geq 2$. For example, if we let $n = 2$, then $2^3 - 3(2)^2 - 9 = -13 < 0$.

<u>Flawed Proof 1</u>

[The given has not been stated. The statement that is to be proven has not been stated. Parts (b) and (e) have been omitted.]

(a) Let $n = 6$. Then $6^3 - 3(6)^2 - 9 \geq 0$, i.e. $99 \geq 0$. **[As in our proof given above, checking the case $n = 6$ is sufficient to prove part (a). However, this proof has not demonstrated this sufficiency. Lastly, no indication has been given that the proof has ended.]**

[The statement that is to be shown has not been stated.]

(c) Let $n = 10$. Then $10^3 - 3(10)^2 - 9 \geq 0$, i.e. $691 \geq 0$. **[Checking the case $n = 10$ is sufficient to prove part (c). However, this sufficiency has not been demonstrated.]**

[The statement that is to be shown has not been stated.]

(d) Let $n = 4$. Then $4^3 - 3(4)^2 - 9 \geq 0$, i.e. $7 \geq 0$. **[Checking the case $n = 4$ is sufficient to prove part (d). However, this sufficiency has not been demonstrated.]**

<u>Flawed Proof 2</u>

[Parts (b),(d) and (e) have been omitted. What is the domain of n?]

(a) It is given that $n \geq 6$. We will prove that $n^3 - 3n^2 - 9 \geq 0$.

Proof. Assume that $n^3 - 3n^2 - 9 \geq 0$. **[In a proof, one should not assume the thing that is to be proven. One needs to show that the given information logically implies the conclusion. In this proof, the reasoning that is presented can mostly be reversed, so that the assumption does in fact apply the conclusion. However, this proof does not explicitly demonstrate knowledge that such a reversal can be done. Also, there is a gap in the reasoning below, which further complicates**

matters.] Adding 9 to both sides, we get $n^3 - 3n^2 \geq 9$. That is, $n^2(n-3) \geq 9$. Taking the minimum possible n, which will produce the minimum possible value in our inequality, we get $6^2(6-3) \geq 9$. [**The previous sentence is true, but it has not been proven.**] That is, $36 \cdot 3 \geq 9$. $\square$

(c) Yes, the inequality holds, since it is true for $n \geq 6$, and the quantity $n^3 - 3n^2 - 6$ will only increase as n increases. [**This assertion is true for $n \geq 6$, but it has not been proven.**]

Flawed Proof 3

[**Parts (b) (c) and (e) have been omitted.**]

(a) We show that $n^3 - 3n^2 - 9 \geq 0$ for $n \geq 6$. [**Actually, we may assume $n \in \mathbb{Z}$, but this is not really necessary. A similar omission is made in the following sentence.**]

We prove the contrapositive statement: if $n < 6$ then $n^3 - 3n^2 - 9 < 0$. Let $n < 6, n \in \mathbb{N}$. [**Actually, we need to assume $n \in \mathbb{Z}$. Moreover, this is not the contrapositive.**] Then $n^3 < 6n^2$ **multiplying both sides by** $n^2 \geq 0$, so $n^3 - 6n^2 < 0$. Adding $3n^2$ to both sides, $n^3 - 3n^2 < 3n^2$. Adding -9 to both sides, $n^3 - 3n^2 - 9 < 3n^2 - 9$, so $n^3 - 3n^2 - 9 < 3(n^2 - 3)$, so $n^3 - 3n^2 - 9 < 3(n - \sqrt{3})(n + \sqrt{3})$. [**Nothing more is written, and the desired assertion has not been proven. Moreover, the end of the proof has not been indicated**]

(d) No, the inequality does not hold for $n \geq 4$ because 5 is not in the original statement. [**Yes, 5 is not in the original statement, but this fact does not answer the question that is asked.**] However, the values for $n \geq 4$ still make the inequality greater than 0. [**The previous sentence is true, but it has not been proven.**]

7. Homework 7

7.1. **Problem 1.** In class, we proved that $\sqrt{2}$ is an irrational number. The proof was by contradiction. In this proof, we first assumed that $\sqrt{2} = n/m$ where n/m is a fraction in lowest terms (i.e. n, m are integers that are relatively prime and $m \neq 0$.) We explain why this assumption was made, and why it is not enough to assume that n and m are integers for which $m \neq 0$.

In the beginning of the proof, we assume for the sake of contradiction that $\sqrt{2} = n/m$, with n, m integers such that n, m are relatively prime and $m \neq 0$. Near the end of the proof, we conclude that 2 divides n, and 2 divides m. That is, there exist $n', m' \in \mathbb{Z}$ such that $n = 2n'$ and $m = 2m'$. In particular, n and m are not relatively prime, and we have reached a contradiction. If we began the proof with the assumption $\sqrt{2} = n/m$ with n, m integers and $m \neq 0$, then we could run the proof again and similarly conclude the following. There exist $n', m' \in \mathbb{Z}$ such that $n = 2n'$ and $m = 2m'$. However, there is no contradiction that is reached, because, a priori, n and m could be any integers (with $m \neq 0$). Nevertheless, we have shown that $\sqrt{2} = n/m = n'/m'$, and n', m' are integers such that $n' = n/2$ and $m' = m/2$. So, if we run the argument with n', m' in place of n, m, we can again pull out a factor of two from n', m'. Iterating this process over and over, we must reach a contradiction. Suppose there exists $N \in \mathbb{Z}$ with $|n| < 2^N$, so that $\log_2 |n| < N$. Since we pull out a factor of 2 from n at each iteration of the argument, we can only iterate the argument at most N times before we reach a contradiction as above.

7.2. **Problem 2.** We prove that $\sqrt{3}$ is an irrational number.
See Problem 4.4(c).

7.3. **Problem 3.** We show that there is no smallest positive real number.

Proof. We argue by contradiction. Assume that r is the smallest positive real number. Then $r > 0$ since r is positive. Since r is a real number, $r/2$ is also a real number. Since $r > 0$, $r/2 > 0$. So, $r/2$ is also a positive real number. Since $1/2 < 1$, multiplying both sides of this inequality by $r > 0$ shows, $r/2 < r$. So r is not the smallest positive real number. Since we have reached a contradiction, we are done. There is no smallest positive real number. □

7.4. **Problem 4.** Let S be a set of elements, and let $*$ be a (binary) operation that is defined for any two elements of S. That is, if $a, b \in S$, then $a * b \in S$. For example, addition is a binary operation on the set of integers, since $a, b \in \mathbb{Z}$ implies that $a + b \in \mathbb{Z}$. An operation $*$ is called commutative if: for all $a, b \in S$, $a * b = b * a$. An operation $*$ is called associative if: for all $a, b \in S$, $(a * b) * c = a * (b * c)$.

(a) We give an example of an operation that is both commutative and associative. Let $S = \mathbb{Z}$, let $a, b \in S$, and define $a * b$ so that $a * b = a + b$. We first prove commutativity.

Proof. Let $a, b \in S$. Then

$$\begin{aligned} a * b &= a + b \quad &&\text{, by the definition of } * \\ &= b + a &&\text{, by commutativity of } + \\ &= b * a &&\text{, by the definition of } * \end{aligned}$$

Thus, for all $a, b \in S$, $a * b = b * a$, i.e. $*$ is commutative for the set S. □

We now prove associativity of $*$ on S.

Proof. Let $a, b, c \in S$. Then

$$\begin{aligned} (a * b) * c &= (a + b) + c \quad &&\text{, by the definition of } * \\ &= a + (b + c) &&\text{, by associativity of } + \\ &= a * (b * c) &&\text{, by the definition of } * \end{aligned}$$

Thus, for all $a, b, c \in S$, $(a * b) * c = a * (b * c)$, i.e. $*$ is commutative for the set S. □

(b) We give an example of an operation that is neither commutative nor associative. Let $S = \mathbb{Z}$, let $a, b \in S$, and define $a * b$ so that $a * b = a - b$. To see that $*$ is not commutative on S, consider $a = 0, b = 1$. By the definition of $*$, $a * b = 0 - 1 = -1$. However, by the definition of $*$, $b * a = 1 - 0 = 1$. So, for $a = 0, b = 1$, $a * b \neq b * a$, i.e. the negation of the commutativity property is true. Therefore, $*$ is not commutative on S. To see that $*$ is not associative on S, consider $a = 0, b = 0, c = 1$. By the definition of $*$, $(a * b) * c = (0 - 0) - 1 = -1$. Also, by the definition of $*$, $a * (b * c) = 0 - (0 - 1) = 1$. So, for $a = 0, b = 0, c = 1$, $a * (b * c) \neq (a * b) * c$, i.e. the negation of the associativity property is true. Therefore, $*$ is not associative on S.

(c) We give an example of an operation that is commutative but not associative. Let $S = \mathbb{Z}$, let $a, b \in S$, and define $a * b$ so that $a * b = a^2 b^2$. To see that $*$ is not associative, let $a = 1, b = 2, c = 2$. Then $a * (b * c) = 1^2 (2^2 2^2)^2 = 2^8 = 256$. However, $(a * b) * c = (1^2 2^2)^2 2^2 = 2^6 = 64$. So, for $a = 1, b = 2, c = 2$, $a * (b * c) \neq (a * b) * c$, i.e. the negation of the associativity property is true. Therefore, $*$ is not associative on S. We now prove that $*$ is commutative on S.

Proof. Let $a, b \in S$. Then

$$\begin{aligned} a * b &= a^2 b^2 && \text{, by the definition of } * \\ &= b^2 a^2 && \text{, by commutativity of multiplication in } \mathbb{Z} \\ &= b * a && \text{, by the definition of } * \end{aligned}$$

Thus, for all $a, b \in S$, $(a * b) = (b * a)$, i.e. $*$ is commutative for the set S. $\square$

(d) We describe an example of an operation that is associative but not commutative. Let S be the set of real 2×2 matrices. That is,

$$S = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : a, b, c, d \in \mathbb{R} \right\}$$

Let $a, b, c, d, e, f, g, h \in \mathbb{R}$. Recall that multiplication on S is defined by

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} e & f \\ g & h \end{bmatrix} = \begin{bmatrix} ae + bg & af + bh \\ ce + dg & cf + dh \end{bmatrix}$$

Let $*$ be multiplication on S. To see that $*$ is not commutative, observe the following example

$$\begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \neq \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix}$$

Thus, the negation of commutativity is true, i.e. $*$ is not commutative for the set S.

We now prove that $*$ is associative on S.

Proof. Let $A, B, C \in S$. Then there exist $a, b, c, d, e, f, g, h, w, x, y, z \in \mathbb{R}$ such that

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}, \qquad B = \begin{bmatrix} e & f \\ g & h \end{bmatrix}, \qquad C = \begin{bmatrix} w & x \\ y & z \end{bmatrix}$$

Observe

$$\begin{aligned} (A * B) * C &= \left(\begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} e & f \\ g & h \end{bmatrix} \right) \begin{bmatrix} w & x \\ y & z \end{bmatrix} && \text{, by the definition of } * \\ &= \begin{bmatrix} ae + bg & af + bh \\ ce + dg & cf + dh \end{bmatrix} \begin{bmatrix} w & x \\ y & z \end{bmatrix} \\ &= \begin{bmatrix} (ae + bg)w + (af + bh)y & (ae + bg)x + (af + bh)z \\ (ce + dg)w + (cf + dh)y & (ce + dg)x + (cf + dh)z \end{bmatrix} \\ &= \begin{bmatrix} a(ew + fy) + b(gw + hy) & a(ex + fz) + b(gx + hz) \\ c(ew + fy) + d(gw + hy) & c(ex + fz) + d(gx + hz) \end{bmatrix} \\ &\quad \text{, by distributivity and associativity of } +, \cdot \text{ on } \mathbb{R} \\ &= \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} ew + fy & ex + fz \\ gw + hy & gx + hz \end{bmatrix} \\ &= \begin{bmatrix} a & b \\ c & d \end{bmatrix} \left(\begin{bmatrix} e & f \\ g & h \end{bmatrix} \begin{bmatrix} w & x \\ y & z \end{bmatrix} \right) \\ &= A * (B * C) && \text{, by the definition of } * \end{aligned}$$

Therefore, for all $A, B, C \in S$, $A * (B * C) = (A * B) * C$, i.e. $*$ is associative on S. $\square$

(e) For each of the following operations, we determine associativity and commutativity.

(e.1) For $a, b \in \mathbb{R}$, define $a * b = (a + b)/2$. We claim that $*$ is commutative, but not associative. To see that $*$ is not associative on $\mathbb{R}$, let $a = b = 0, c = 1$. Then $a * (b * c) = a * ((0+1)/2) = a * (1/2) = (0+1/2)/2 = 1/4$. However, $(a*b)*c = 0*c = (0+1)/2 = 1/2$. Since $1/2 \neq 1/4$, we conclude that $(a*b)*c \neq a*(b*c)$, i.e. the negation of the associativity property is true. Therefore, $*$ is not associative on $\mathbb{R}$. We now prove that $*$ is commutative on $\mathbb{R}$.

Proof. Let $a, b \in \mathbb{R}$. Observe

$$\begin{aligned} a * b &= (a + b)/2 && \text{, by definition of } * \\ &= (b + a)/2 && \text{, by commutativity of addition on } \mathbb{R} \\ &= b * a && \text{, by definition of } * \end{aligned}$$

So, for all $a, b \in \mathbb{R}$, $a * b = b * a$, i.e. $*$ is commutative on $\mathbb{R}$. $\square$

(e.2) For $a, b \in \mathbb{N}$, define $a * b = a^b$. We claim that $*$ is not commutative, and $*$ is not associative. To see that $*$ is not commutative on $\mathbb{N}$, let $a = 1, b = 2$. Then $a * b = 1^2 = 1 \neq 2 = 2^1 = b * a$, i.e. the negation of the commutativity property is true, so $*$ is not commutative on $\mathbb{N}$. To see that $*$ is not associative, let $a = 2, b = 1, c = 2$. Then $a * (b * c) = a * (1^2) = a * 1 = 2^1 = 2 \neq 4 = 2^2 = 2 * c = (2^1) * c = (a * b) * c$, i.e. the negation of the associativity property is true. Therefore, $*$ is not associative on $\mathbb{N}$.

(e.3) For $a, b \in \mathbb{Q}$, define $a*b = b$. We claim that $*$ is not commutative, and $*$ is associative. To see that $*$ is not commutative on $\mathbb{Q}$, let $a = 0, b = 1$. Then $a * b = 1 \neq 0 = b * a$, i.e. the negation of the commutativity property is true. Therefore, $*$ is not commutative on $\mathbb{Q}$. We now prove that $*$ is associative on $\mathbb{Q}$.

Proof. Let $a, b, c \in \mathbb{Q}$. Observe

$$\begin{aligned} a * (b * c) &= a * c && \text{, by definition of } * \\ &= c && \text{, by definition of } * \\ &= b * c && \text{, by definition of } * \\ &= (a * b) * c && \text{, by definition of } * \end{aligned}$$

So, for all $a, b, c \in \mathbb{Q}$, $a * (b * c) = (a * b) * c$, i.e. $*$ is associative on $\mathbb{Q}$. $\square$

8. Homework 8

8.1. **Problem 1.** In the following problem, we make use of the following facts.

(i) If two sides of a triangle are equal, then the measures of the angles opposite these sides are equal.
(ii) If two angles of a triangle are equal, then the lengths of the sides opposite these angles are equal. (This is the converse of (i).)
(iii) An exterior angle of a triangle is larger than any interior angle that is not adjacent to that exterior angle.

If a triangle has edges A, B, we denote the angle created by the edges A, B with the notation $\angle AB$. We denote the measure of such an angle $\angle AB$ with the notation $m\angle AB$.

8.1.1. Suppose we have a triangle with edges A, B, C and corresponding edge lengths $a, b, c > 0$. Suppose also that $a > b$. We prove that, as a result, $m\angle BC > m\angle AC$.

Proof. Extend side C to create a new triangle with edges A, B', C' with corresponding edge lengths $a, b', c' > 0$, so that $b' = a$. By Fact (i), $m\angle AC' = m\angle B'C'$. By Fact (iii), $m\angle BC > m\angle B'C'$. Since C' extends C, $m\angle AC = m\angle AC'$. Combining these observations, $m\angle BC > m\angle B'C' = m\angle AC' = m\angle AC$, as desired. □

8.1.2. Suppose we have a triangle with edges A, B, C and corresponding edge lengths $a, b, c > 0$. Suppose also that $m\angle BC > m\angle AC$. We prove that, as a result, $a > b$.

Proof. We argue by contradiction. Suppose $a \leq b$. If $a = b$, then $m\angle BC = m\angle AC$ by Fact (i), violating our assumption that $m\angle BC > m\angle AC$. We therefore assume that $a < b$. Extend side A to create a new triangle with edges A', B', C with corresponding edge lengths a', b', c, so that $a' = b'$. Since the new triangle is constructed by extending the side A, the new triangle strictly contains the old triangle. By this strict containment, $m\angle B'C > m\angle BC$. By Fact (i), $m\angle A'C = m\angle B'C$. Since the new triangle was contructed by extending A and leaving the edge C alone, $m\angle AC = m\angle A'C$. Combining these observations, $m\angle AC = m\angle A'C = m\angle B'C > m\angle BC$, i.e. our assumption has been violated. Since we have achieved a contradiction, we must conclude that $a > b$, as desired. □

8.1.3. Suppose we have a (nontrivial) triangle with edges A, B, C and corresponding edge lengths $a, b, c > 0$. Using our observations above, we prove that $b + c > a$.

Proof. Extend side C at the vertex corresponding to $\angle BC$. Specifically, extend C by adding a segment B' of length b. Let E be the union of segments C and B'. Form a new triangle with the edges A and E. Label the third edge of this new triangle as D. Consider the triangle with edges B, B' and D. Since the segments B and B' are of equal length, Fact (i) says $m\angle BD = m\angle B'D$. Since the edges E, D create the same angle as the edges B', D, $m\angle ED = m\angle B'D$. Since the triangle with edges A, E, D strictly contains the triangle with edges B, B', D, we conclude that $m\angle AD > m\angle BD$. Combining these observations, $m\angle AD > m\angle ED$. So, from Problem 8.1.2, the length of A is less than the length of E, i.e. $a < b + c$, as desired. □

Note that, by relabeling the edges of the given triangle, we can conclude that $a + b > c$ and $a + c > b$.

8.2. **Problem 2.**

8.2.1. In Problem 4.4(c), we showed: for a prime P, $\sqrt{P}$ is an irrational number. We explain why this proof does not apply for the case $P = 4$.

In the proof, we have positive integers p and q. We then have an expression of the form $p^2 = Pq^2$. We then asserted that P divides p, i.e. there exists a positive integer M such that $p = PM$. If P is a prime, this assertion is justified by the Fundamental Theorem of Arithmetic. However, in the case $P = 4$, this assertion is not true. For example, let $p = 2, q = 1$. Then $p^2 = 4q^2$. However, 4 does not divide p, i.e. there does not exist a positive integer N such that $p = 4N$. Due to this issue, the argument cannot proceed.

8.2.2. We prove that $\sqrt{6}$ is an irrational number.

Proof. The argument is essentially identical to that of Problem 4.4(c). We note the necessary changes. Within the proof, we have positive integers p, q and we arrive at an expression of the form $p^2 = 6q^2$. Since $6 = 2 \cdot 3$, and since 2 and 3 are distinct primes, the Fundamental Theorem of Arithmetic implies that both 2 and 3 divide p. Therefore, there exists a positive integer M such that $p = 6M$. Continuing the argument of Problem 4.4(c), we conclude that 6 also divides q. So, p and q both have 6 as a divisor. The rest of the argument of Problem 4.4(c) continues unchanged. □

8.2.3. Let p, q be irrational numbers. We show that $p \cdot q$ can be rational.

We first claim the following. If p is irrational, then $1/p$ is irrational. (Since p is irrational, $p \neq 0$, so $1/p$ is defined.)

Proof. We argue by contradiction. Suppose $1/p$ is rational. Then we can write $1/p = m/n$ with $m, n \in \mathbb{Z}$, $m \neq 0, n \neq 0$. But then $p = n/m$, i.e. p is rational. Since we have contradicted our assumption that p is irrational, we must conclude that $1/p$ is irrational. □

Using our claim, let p be irrational, and let $q = 1/p$, so that q is also irrational. Note that $p \cdot q = 1$, i.e. $p \cdot q$ may be rational, as desired.

8.2.4. We show that $\sqrt{2} + \sqrt{3}$ is an irrational number.

Proof. We argue by contradiction. Suppose $\sqrt{2} + \sqrt{3}$ is rational. Then there exist $n, m \in \mathbb{Z}$, $n \neq 0$ such that $\sqrt{2} + \sqrt{3} = m/n$. Squaring both sides of this expression gives $2 + 3 + 2\sqrt{6} = m^2/n^2$, i.e. $\sqrt{6} = (m^2/2n^2) - 1 - 3/2 = (m^2 - 2n^2 - 3n^2)/(2n^2) \in \mathbb{Q}$, contradicting Problem 8.2.2. Since we have achieved a contradiction, we conclude that $\sqrt{2} + \sqrt{3}$ is irrational. □

8.2.5. We show that the sum of two irrational numbers can be rational.

We begin with a claim: if p is an irrational number, then $-p$ is an irrational number.

Proof. We argue by contradiction. Suppose $-p$ is rational. Then there exist $n, m \in \mathbb{Z}$, $n \neq 0$ such that $-p = m/n$. But then $p = (-m)/n$, $-m \in \mathbb{Z}, n \in \mathbb{Z}$, i.e. p is rational. Since this statement contradicts the irrationality of p, we conclude that $-p$ must be irrational. □

Given this claim, let p be irrational, so that $-p$ is also irrational. Then $p + (-p) = 0 \in \mathbb{Q}$, i.e. the sum of two irrational numbers can be rational.

8.2.6. We show that $\sqrt{2} + 8$ is irrational.

Let $p = \sqrt{2}$, let $q = 8$, note that $\sqrt{2}$ is irrational and apply Problem 8.2.7.

8.2.7. Let p be irrational and let q be rational, so that there exist $a, b \in \mathbb{Z}$ with $b \neq 0$ such that $q = a/b$. We prove that $p + q$ is irrational.

Proof. We argue by contradiction. Suppose $p + q$ is rational. Then there exist $n, m \in \mathbb{Z}$, $n \neq 0$ such that $p + q = m/n$. But then $p = (m/n) - q = (m/n) - (a/b) = (mb - an)/nb \in \mathbb{Q}$, contradicting that p is irrational. Since we have achieved a contradiction, we must conclude that $p + q$ is irrational. □

8.2.8. We prove that $(5/9)\sqrt{2}$ is irrational.

Proof. We argue by contradiction. Suppose $(5/9)\sqrt{2}$ is rational. Then there exist $n, m \in \mathbb{Z}$, $n \neq 0$ such that $(5/9)\sqrt{2} = m/n$. But then $\sqrt{2} = (9m)/(5n) \in \mathbb{Q}$, contradicting the irrationality of $\sqrt{2}$. Due to this contradiction, we conclude that $(5/9)\sqrt{2}$ is irrational. □

8.2.9. We show that the product of an irrational number and a rational number can be rational.

Let $p = \sqrt{2}$ and let $q = 0$. Then p is irrational, q is rational, and $p \cdot q = 0$ is rational.

8.2.10. We show that the set $\{a + b\sqrt{2} \colon a, b \in \mathbb{Q}, b \neq 0\}$ consists entirely of irrational numbers.

We begin with the following claim. If p is irrational and q is rational with $q \neq 0$, then $p \cdot q$ is irrational.

Proof. We argue by contradiction. Suppose $p \cdot q$ is rational. Then there exist $n, m \in \mathbb{Z}$, $n \neq 0$ such that $p \cdot q = m/n$. Since q is rational and nonzero, there exist $a, b \in \mathbb{Z}$, $a \neq 0, b \neq 0$ such that $q = a/b$. But then $p = (bm)/(an) \in \mathbb{Q}$, contradicting the irrationality of p. Since we have achieved a contradiction, we must conclude that $p \cdot q$ is irrational. □

With the claim in hand, we can prove that the set $\{a + b\sqrt{2} \colon a, b \in \mathbb{Q}, b \neq 0\}$ consists entirely of irrational numbers.

Proof. Let $a, b \in \mathbb{Q}, b \neq 0$. Since $\sqrt{2}$ is irrational, the claim shows that $b\sqrt{2}$ is irrational. Since $a \in \mathbb{Q}$ and $b\sqrt{2}$ is irrational, Problem 8.2.7 shows that $a + b\sqrt{2}$ is irrational. □

8.2.11. Consider the set of numbers of the form $a + b\sqrt{2}$ where $a, b \in \mathbb{Q}$ and at least one of a, b is nonzero. We find necessary and sufficient conditions on $a, b \in \mathbb{Q}$ so that $a + b\sqrt{2}$ is irrational.

From Problem 8.2.10, the set $\{a + b\sqrt{2} \colon a, b \in \mathbb{Q}, b \neq 0\}$ consists entirely of irrational numbers. Given $a, b \in \mathbb{Q}$, if $b = 0$, then $a + b\sqrt{2} = a \in \mathbb{Q}$. Since we have covered all cases of $a, b \in \mathbb{Q}$, we are done.

8.3. **Problem 3.** Let $(G, *)$ be a group. That is, G is a set, and $*$ is an operation that satisfies the following four conditions.

(i) If $a, b \in G$, then $a * b \in G$. (So, $*$ is a binary operation on G.)
(ii) If $a, b, c \in G$ then $(a * b) * c = a * (b * c)$. (So, $*$ is associative on G.)
(iii) $\exists\, e \in G$ such that, $\forall\, g \in G$, $e * g = g * e = g$. (So, $(G, *)$ has an identity element e.)
(iv) $\forall\, g \in G$, $\exists\, g' \in G$ such that $g * g' = g' * g = e$. (Every element of G has an inverse.)

8.3.1. We give an example of a group, and we show that it satisfies the four conditions of the definition of a group.

Let G be the set of positive rational numbers, and let $*$ denote the usual multiplication on rational numbers.

We prove that Property (i) holds.

Proof. Let $a, b \in G$. Then there exist $p, q, x, y \in \mathbb{Z}$ with $p, q, x, y > 0$ such that $a = p/q$ and $b = x/y$. Since $p, q, x, y \in \mathbb{Z}$, $px, qy \in \mathbb{Z}$. Since $p, q, x, y > 0$, $px, qy > 0$. So, $(px)/(qy) \in \mathbb{Q}$ and $(px)/(qy) > 0$. So, $a * b = (p/q)(x/y) = (px)/(qy) \in G$, i.e. Property (i) has been verified. □

We prove that Property (ii) holds.

Proof. Let $a, b, c \in G$. Since $a, b, c \in \mathbb{Q}$, and since $*$ is the usual multiplication on $\mathbb{Q}$, associativity of $*$ follows directly from associativity of multiplication on $\mathbb{Q}$. $\square$

We prove that Property (iii) holds.

Proof. Let $g \in G$, and define $e = 1$. Since 1 is a positive rational, $e \in G$. Also, $e*g = 1 \cdot g = g$, and $g * e = g \cdot 1 = g$, as desired. $\square$

We prove that Property (iv) holds.

Proof. Let $g \in G$. Since $g > 0$, there exists $m, n \in \mathbb{Z}$ with $m, n > 0$ such that $g = m/n$. Define $g' = n/m$. Since $n, m > 0$ and $n, m \in \mathbb{Z}$, we know that $g' \in G$. Now, by definition of $*$ and e we have $g * g' = (mn)/(nm) = 1 = e$, and $g' * g = (nm)/(mn) = 1 = e$, so Property (iv) has been verified. $\square$

8.3.2. Let G be the set of numbers defined in Problem 8.2.11. Let $\times$ be the usual operation of multiplication of real numbers. We show that $(G, \times)$ is a group.

Proof. Let $x, y \in G$. Then there exist $a, b, c, d \in \mathbb{Q}$ such that $x = a + b\sqrt{2}$, $y = c + d\sqrt{2}$, at least one of a, b is nonzero, and at least one of c, d is nonzero. We prove Properties (i) through (iv) in succession.

To prove Property (i), we need to show that $x \times y \in G$. Observe

$$x \times y = (ac + 2bd) + (ad + bc)\sqrt{2}$$

To show that $x \times y \in G$, it remains to show: either $ac + 2bd \neq 0$ or $ad + bc \neq 0$. To show this, we argue by contradiction. Suppose $ac + 2bd = 0$ and $ad + bc = 0$. Then $ac = -2bd$ and $ad = -bc$, so $acd = -2bd^2$, so $(ad)c = -2bd^2$ so $-bc^2 = -2bd^2$. If $b = 0$, then $ac = 0$, $ad = 0$. Also, if $b = 0$, then $x = a + b\sqrt{2} \in G$, so $a \neq 0$, so $c = d = 0$, contradicting that $y = c + d\sqrt{2} \in G$. Therefore, b must be nonzero. Since $-bc^2 = -2bd^2$, we conclude that $c^2 = 2d^2$. If $c = 0$, then $d = 0$, contradicting that $y \in G$. So $c \neq 0$ and $d \neq 0$. But then $|c| = \sqrt{2}\,|d|$, and $|c|, |d| \in \mathbb{Q}$. Also, $\sqrt{2}$ is irrational. Thus, the claim of Problem 8.2.10 has been violated. Since we have achieved a contradiction, we must assume: either $ac + 2bd \neq 0$ or $ad + bc \neq 0$. In summary, $x \times y \in G$, and Property (i) has been verified.

We now prove Property (ii). Since $\times$ is given by multiplication of real numbers, associativity of $\times$ follows directly from associativity of multiplication of real numbers.

We now prove Property (iii). Let $a = 1, b = 0$. Note that $a, b \in \mathbb{Q}$ and $a \neq 0$. Define $e = a + b\sqrt{2}$, and note that $e \in G$. Moreover, since $e = 1$, $x \times 1 = x$ and $1 \times x = x$, i.e. Property (iii) has been verified.

We finally prove Property (iv). As above, let $x = a + b\sqrt{2}$ with $a, b \in \mathbb{Q}$, and such that at least one of a, b is nonzero. Since $a, b \in \mathbb{Q}$, $a^2 - 2b^2 \in \mathbb{Q}$. We claim that $a^2 - 2b^2 \neq 0$. To see this, we argue by contradiction. Assume $a^2 - 2b^2 = 0$, i.e. $a^2 = 2b^2$. Then $|a| = \sqrt{2}\,|b|$. Since at least one of a, b is nonzero, we conclude that both $|a|$ and $|b|$ are nonzero rational numbers. Since $|a| = \sqrt{2}\,|b|$, the Claim of Problem 8.2.10 has been violated. Since we have arrived at a contradiction, we conclude that $a^2 - 2b^2 \neq 0$.

Now, since $a^2 - 2b^2$ is nonzero and in $\mathbb{Q}$, we get that $a/(a^2 - 2b^2) \in \mathbb{Q}$, $-b/(a^2 - 2b^2) \in \mathbb{Q}$. Define $x' = (a/(a^2 - 2b^2)) + (-b/(a^2 - 2b^2))\sqrt{2}$. Note that $x' \in G$ since $a^2 - 2b^2 \neq 0$, and at least one of a, b is nonzero (since $x = a + b\sqrt{2} \in G$.) Observe

$$x \times x' = (a + b\sqrt{2}) \left(\frac{a}{a^2 - 2b^2} - \frac{b}{a^2 - 2b^2}\sqrt{2} \right) = \frac{a^2 - 2b^2}{a^2 - 2b^2} + \frac{ab\sqrt{2}}{a^2 - 2b^2} - \frac{ab\sqrt{2}}{a^2 - 2b^2} = 1 = e$$

And since $\times$ is given by the usual multiplication on real numbers, $\times$ is commutative, so $x' \times x = x \times x' = e$, i.e. Property (iv) has been verified.

Since Properties (i) through (iv) have been verified, we conclude that $(G, \times)$ is a group. $\square$

9. Homework 9

9.1. **Problem 1.** For $n \in \mathbb{N}$, define $a_n = n(n+1)/2$. We give explicit formulas for certain elements of this sequence.

$$a_{n+1} = \frac{(n+1)(n+2)}{2}, \quad a_{n-1} = \frac{(n-1)n}{2}, \quad a_{n+5} = \frac{(n+5)(n+6)}{2}, \quad a_{2n-1} = (2n-1)n$$

9.2. **Problem 2.** For $n \in \mathbb{N}$, define $a_n = 3^{2n-1}/4^n$. We give explicit formulas for certain elements of this sequence.

$$a_{n+1} = \frac{3^{2n+1}}{4^{n+1}}, \quad a_{n-1} = \frac{3^{2n-3}}{4^{n-1}}, \quad a_{n+5} = \frac{3^{2n+9}}{4^{n+5}}, \quad a_{2n-1} = \frac{3^{4n-3}}{4^{2n-1}}$$

9.3. **Problem 3.** For $n \in \mathbb{N}$, define $\sigma_n = 1/(n+1) + 1/(n+2) + \cdots + 1/(2n)$.

9.3.1. We give explicit formulas for certain elements of this sequence.

$$\sigma_{n+1} = \frac{1}{n+2} + \frac{1}{n+3} + \cdots + \frac{1}{2n+2}, \quad \sigma_{n+2} = \frac{1}{n+3} + \frac{1}{n+4} + \cdots + \frac{1}{2n+4}$$

9.3.2. We find a formula for $\sigma_{n+1} - \sigma_n$.

$$\sigma_{n+1} - \sigma_n = \frac{1}{2n+2} + \frac{1}{2n+1} - \frac{1}{n+1}$$

9.4. **Problem 4.** Let $a_1 = 1$, and for $n \in \mathbb{N}$ define $a_n = 3 \cdot a_{n-1}$. We prove that $a_n = 3^{n-1}$.

Proof. We prove the formula for a_n by induction. Note that $a_1 = 3^{1-1} = 3^0 = 1$, so the base case of the induction is known. We now induct on $n \in \mathbb{N}$. Assume that $a_{n-1} = 3^{(n-1)-1} = 3^{n-2}$. To complete the induction, we will show that $a_n = 3^{n-1}$. Since $a_n = 3 \cdot a_{n-1}$, we can apply the induction hypothesis to see that $a_n = 3 \cdot a_{n-1} = 3 \cdot 3^{n-2} = 3^{n-1}$. Since the inductive step has been completed, the assertion is proven. $\square$

9.5. **Problem 5.** Let $b_1 = 3$, and for $n \in \mathbb{N}$ define $b_n = 3 \cdot b_{n-1}$. We prove that $b_n = 3^n$.

Proof. We prove the formula for b_n by induction. Note that $b_1 = 3 = 3^1$, so the base case of the induction is known. We now induct on $n \in \mathbb{N}$. Assume that $b_{n-1} = 3^{n-1}$. To complete the induction, we will show that $b_n = 3^n$. Since $b_n = 3 \cdot b_{n-1}$, we can apply the induction hypothesis to see that $b_n = 3 \cdot b_{n-1} = 3 \cdot 3^{n-1} = 3^n$. Since the inductive step has been completed, the assertion is proven. $\square$

9.6. **Problem 6.** We explain a relation for the sequences defined in Problems 9.4 and 9.5.

These two sequences are the same, if we shift the index element n by 1. However, we have to be careful with the domain of n. We define the natural numbers so that $\mathbb{N} = \{1, 2, 3, \ldots\}$. For $n \in \mathbb{N}$ with $n \geq 1$, we have $a_{n+1} = 3^n = b_n$. (Sometimes the natural numbers are defined to include zero, but in this set of notes we do not do this.) With this definition of the natural numbers, b_n is undefined for $n = 0$, but a_{n+1} is defined.

9.7. **Problem 7.** We prove: $\forall\, n \in \mathbb{N}$, $1 + 3 + 5 + \cdots + (2n - 1) = n^2$.

Proof. Let $a_1 = 1$, and for $n \in \mathbb{N}$, let $a_n = 1 + 3 + \cdots + (2n - 1)$. We show that $a_n = n^2$ by induction on n. Since $a_1 = 1$, the base case is verified. Assume that $a_{n-1} = (n - 1)^2$. To complete the induction, we will show that $a_n = n^2$. Since $a_n = a_{n-1} + (2n - 1)$, we apply the inductive hypothesis to get $a_n = (n - 1)^2 + (2n - 1) = n^2 - 2n + 1 + 2n - 1 = n^2$. Since the inductive step has been completed, the assertion is proven. □

10. Homework 10

10.1. **Problem 1.** In the Towers of Hanoi problem, we are given three pegs A, B, C and n rings ($n \in \mathbb{N}$) of different widths. At the beginning of the problem, all rings lie on peg A. If a ring r_1 lies on top of a ring r_2, then the width of r_1 must be less than that of r_2. So, at the beginning of the problem, the rings sit on peg A with sorted widths. The problem asks if we can transfer all rings from peg A to peg C. In this problem, we say that one move occurs when one ring is transferred from some peg to another different peg.

10.1.1. For any $n \in \mathbb{Z}$, $n \geq 1$, we prove that it is possible to move a tower of n rings from peg A to peg C.

Proof. We prove the assertion by induction on n. In the case $n = 1$, we have only one ring, so we can move this one ring from peg A to peg C, according to the rules of the problem. With the base case proven, we now assume: for a fixed $n \in \mathbb{Z}, n \geq 1$, it is possible to move n rings from peg A to peg C. We now treat the case of $n + 1$ rings. In this case, we first consider the n smallest rings.

We will explicitly describe a method for moving the rings. For now, we will never move the largest ring. Since the largest ring always has the lowest possible position within the problem, and since we leave the largest ring in its initial position, the largest ring can never impede the movement of any smaller ring. That is, we may move the n smallest rings as if we started with only n rings. So, by the inductive hypothesis, we can transfer the n smallest rings from peg A to peg B. (The inductive hypothesis says we can move the n smallest rings from peg A to peg C, but the labels B and C are arbitrary, so we can instead move the n smallest rings from peg A to peg B.)

Now, move the largest ring from peg A to peg C. As before, the largest ring has the lowest possible position within the problem, so we can move the n smallest rings as if we started with only n rings. So, applying the inductive hypothesis again, move the n smallest rings from peg B to peg C. At this point, all rings lie on peg C, implying that their widths must be sorted. So, we have found a way to move $n + 1$ rings from peg A to peg C. Since the inductive step has been completed, the assertion has been proven. □

10.1.2. For $n \in \mathbb{Z}$, $n \geq 1$, we prove that it is possible to move a tower of n rings from peg A to peg C with $2^n - 1$ moves.

Proof. We prove the assertion by induction on n. We use the procedure from Problem 10.1.1. For $n = 1$, the procedure from Problem 10.1.1 moves the single ring from peg A to peg C, resulting in one move. Since $2^1 - 1 = 1$, the base case of the induction is completed. We now assume that, for a fixed $n \in \mathbb{Z}, n \geq 1$, the procedure from Problem 10.1.1 uses $2^n - 1$ moves. We now treat the case of $n + 1$ rings. From the procedure of Problem 10.1.1, we first move the tower of the n smallest rings from peg A to peg B. By the inductive hypothesis, this step requires $2^n - 1$ moves. We then move the largest width ring from peg A to peg C, requiring 1 move. We then move the tower of the n smallest rings from peg B to peg C. Again, by the inductive hypothesis, this step requires $2^n - 1$ moves. The moves have now been completed, and we have used $2(2^n - 1) + 1 = 2^{n+1} - 2 + 1 = 2^{n+1} - 1$ moves. Since the inductive step has been completed, the assertion is proven. $\square$

10.1.3. Suppose we have $n = 64$ rings in the Towers of Hanoi problem, and one move is allowed per day. We show that, if we used the procedure described in Problem 10.1.1, then it would take approximately 5.05×10^{16} years to complete the problem.

Proof. From Problem 10.1.2, it would take $2^{64} - 1$ days to complete the problem. In the Gregorian calendar system, every 400 years have 97 leap years. So, every 400 years have $365 \cdot 400 + 97$ days, i.e. the average year has $365 + (97/400)$ days. So, it would take about $(2^{64} - 1)/(365 + (97/400)) \approx 5.05 \times 10^{16}$ years to complete the problem, which is over 3 million times the age of the universe (estimated at 1.37×10^{10} years). $\square$

10.2. **Problem 2.** For $n \in \mathbb{N}$, $n \geq 3$, we prove that the sum of the interior angles (in radians) of an n-sided convex polygon is $(n - 2)\pi$.

If v, w are the vertices of a polygon, we denote $\overline{vw}$ as the straight line between v and w. By a polygon, we mean a two-dimensional planar region that is bounded by flat one-dimensional edges. A polygon is convex if, given any two points x, y in the polygon, the line $\overline{xy}$ lies inside the polygon.

Proof. We prove the assertion by induction on n. For $n = 3$, we know that the sum of the interior angles of a 3-sided convex polygon (i.e. a triangle) is $\pi = (n - 2)\pi$. Therefore, the base case has been verified. We now assume that the assertion is true for a fixed $n \in \mathbb{N}$, $n \geq 3$. We then consider the case $n + 1$. Suppose v_1, v_2, v_3 are three vertices of an $(n + 1)$-sided convex polygon P such that v_1 is adjacent to v_2, v_2 is adjacent to v_3, and v_1, v_2, v_3 are distinct vertices. Since $n + 1 \geq 4 > 3$, such vertices exist.

Consider the triangle T formed by the vertices v_1, v_2, v_3. This triangle has edges $\overline{v_1v_2}$, $\overline{v_2v_3}$, and $\overline{v_1v_3}$. The first two of these edges belong to P. The third edge lies inside P, since P is convex. Let P' be the polygon formed by removing T from P. Then P' has the same edges as P, except that the edges $\overline{v_1v_2}$, $\overline{v_2v_3}$ have been removed, and the edge $\overline{v_1v_3}$ has been added. Since we have removed two edges and added one, P' has $(n + 1) - 2 + 1 = n$ edges.

In order to apply the inductive hypothesis, we need to show that P' is convex. Let x, y be any two points in P'. Since P' lies inside P, x, y are in P. Since P is convex, the line $\overline{xy}$ lies in P. Assume for the sake of contradiction that $\overline{xy}$ intersects the interior of T. Since x and y lie outside the interior of T, $\overline{xy}$ must enter and exit T through the boundary of T. If $\overline{xy}$ enters and exits T through a single edge of T, then $\overline{xy}$ is also parallel to that edge of T. So,

$\overline{xy}$ avoids the interior of T, a contradiction. If $\overline{xy}$ enters and exits T through two different edges of T, then $\overline{xy}$ crosses either edge $\overline{v_1v_2}$ or edge $\overline{v_2v_3}$. Since these edges are also edges of P, $\overline{xy}$ exits P in both of these cases, contradicting that $\overline{xy}$ lies in P. Since we have achieved a contradiction, we conclude that $\overline{xy}$ does not intersect the interior of T, i.e. $\overline{xy}$ lies in P', so that P' is convex.

We now know that P' is a convex n-sided polygon. By the inductive hypothesis, the sum of the interior angles of P' is $\pi(n-2)$. By the definition of P', the sum of the interior angles of P is the sum of the interior angles of P', plus the sum of the interior angles of T. Since T is a triangle, we conclude that the sum of the interior angles of P is $\pi(n-2)+\pi = \pi(n-1) = \pi((n+1)-2)$. Since the inductive step has been completed, the proof is complete. $\square$

10.3. **Problem 3.** The first few terms of a sequence are given as: $a_1 = 2$, $a_2 = 4$, $a_3 = 8$, $a_4 = 16$, $a_5 = 32$.

10.3.1. We find a rule for a_n, $n \geq 1$, $n \in \mathbb{Z}$.
$a_n = 2^n$.

10.3.2. We find another rule for a_n.
We will find a polynomial in the variable n along with $a, b, c, d, e \in \mathbb{R}$ such that

$$a_n = a + bn + cn^2 + dn^3 + en^4$$

To find $a, b, c, d, e \in \mathbb{R}$, we want the following equations to be satisfied

$$\begin{aligned}
2 &= a + b + c + d + e \\
4 &= a + 2b + 4c + 8d + 16e \\
8 &= a + 3b + 9c + 27d + 81e \\
16 &= a + 4b + 16c + 64d + 256e \\
32 &= a + 5b + 25c + 125d + 625e
\end{aligned}$$

Rewriting this in matrix form,

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 1 \\ 1 & 2 & 4 & 8 & 16 \\ 1 & 3 & 9 & 27 & 81 \\ 1 & 4 & 16 & 64 & 256 \\ 1 & 5 & 25 & 125 & 625 \end{bmatrix} \begin{bmatrix} a \\ b \\ c \\ d \\ e \end{bmatrix} = \begin{bmatrix} 2 \\ 4 \\ 8 \\ 16 \\ 32 \end{bmatrix}$$

Using linear algebra, we can solve this equation for $a, b, c, d, e \in \mathbb{R}$. We get $a = 2, b = -3/2, c = 23/12, d = -1/2, e = 1/12$. Therefore, we can write the following rule for a_n.

$$a_n = 2 - \frac{3}{2}n + \frac{23}{12}n^2 - \frac{1}{2}n^3 + \frac{1}{12}n^4$$

10.3.3. We explain whether or not this sequence is uniquely defined.
The sequence is not uniquely defined. Using our rule from Problem 10.3.1, we get $a_6 = 2 \cdot a_5 = 64$. However, using our rule from Problem 10.3.2, $a_6 = 62 \neq 64$.

10.4. **Problem 4.** For all $n \in \mathbb{Z}$, $n \geq 1$, define $a_n = 10^n - 7$.

10.4.1. We prove: if a_n is divisible by 9, then a_{n+1} is also divisible by 9.

Proof. Let $n \in \mathbb{N}$. Suppose $a_n = 9k$, $k \in \mathbb{Z}$. That is, $10^n - 7 = 9k$. Then

$$a_{n+1} = 10^{n+1} - 7 = (9+1) \cdot 10^n - 7 = 9 \cdot 10^n + 10^n - 7 = 9 \cdot 10^n + a_n = 9(10^n + k)$$

Since $10^n \in \mathbb{Z}$ and $k \in \mathbb{Z}$, $10^n + k \in \mathbb{Z}$, i.e. there exists $j \in \mathbb{Z}$ such that $a_{n+1} = 9j$. Therefore, a_{n+1} is divisible by 9. □

10.4.2. We show that for all $n \in \mathbb{Z}$ with $n \geq 1$, a_n is not divisible by 9.

Proof. By the definition of a_n, a_n is a number of the form $99\ldots93$. In particular, for $n \in \mathbb{Z}, n \geq 1$, the second through n^{th} digit of a_n is 9, and the first digit of a_n is 3. From the divisibility by 9 rule, a_n is divisible by 9 if and only if the sum of the digits of a_n is divisible by 9. However, the sum of the digits of a_n is $(n-1)9 + 3$, which is not divisible by 9. Therefore, a_n is not divisible by 9. □

11. Homework 11

Part 2: An Incomplete Proof. We show that, $\forall\, n \in \mathbb{N}$, $1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$.

Proof. We prove this assertion by induction on n. We begin with the base case, $n = 1$. In this case, the left side of the desired equality is $1^2 = 1$, and the right side is $1 \cdot 2 \cdot 3/6 = 1$. Since both sides of the desired equality are equal to 1, the base case has been verified. For good measure, we also check the case $n = 2$. In this case, the left side of the desired equality is $1^2 + 2^2 = 5$, and the right side is $2 \cdot 3 \cdot 5/6 = 5$. Since both sides of the desired equality are equal to 5, the case $n = 2$ has been verified.

We now begin the inductive step. Assume that, for $k \in \mathbb{N}$ we have $1^2 + 2^2 + \cdots + k^2 = k(k+1)(2k+1)/6$. We will show that $1^2 + 2^2 + \cdots + k^2 + (k+1)^2 = (k+1)(k+2)(2k+3)/6$. Observe

$$\begin{aligned} 1^2 + 2^2 + \cdots + k^2 + (k+1)^2 &= \frac{k(k+1)(2k+1)}{6} + (k+1)^2 \quad \text{, by the inductive hypothesis} \\ &= \frac{k(k+1)(2k+1) + 6(k+1)^2}{6} = \frac{2k^3 + 9k^2 + 13k + 6}{6} \\ &= \frac{(k+1)(k+2)(2k+3)}{6} \quad \text{, by algebra} \end{aligned}$$

We conclude that $1^2 + 2^2 + \cdots + k^2 + (k+1)^2 = (k+1)(k+2)(2k+3)/6$, completing the inductive step. Since the inductive step has been completed, the proof is complete. □

11.1. **Problem 1.** We show: $\forall\, n \in \mathbb{N}$, $1 + 2 + 4 + \cdots + 2^n = 2^{n+1} - 1$.

Proof. For $n \in \mathbb{N}$, let $a_n = 1 + 2 + 4 + \cdots + 2^n$. We prove the desired equality $a_n = 2^{n+1} - 1$ by induction. We begin with the base case. In this case, $a_1 = 1 + 2 = 2^2 - 1$. Since the base case has been verified, we begin with the inductive step. For fixed $n \in \mathbb{N}$, assume that $a_n = 2^{n+1} - 1$. We now prove that $a_{n+1} = 2^{n+2} - 1$. Since $a_{n+1} = a_n + 2^{n+1}$, we can substitute in the inductive hypothesis to show that

$$a_{n+1} = (2^{n+1} - 1) + 2^{n+1} = 2(2^{n+1}) - 1 = 2^{n+2} - 1$$

Since the inductive step has been completed, the proof is complete. □

11.2. **Problem 2.** We prove: $\forall\, n \in \mathbb{N}$, $10^n - 1$ is divisible by 9.

Proof. Let $n \in \mathbb{N}$, and define $a_n = 10^n - 1$. Using induction, we will show that a_n is divisible by 9, for all $n \in \mathbb{N}$. Since $a_1 = 9$, we know that a_1 is divisible by 9. With the base case completed, we proceed to the inductive step. For fixed $n \in \mathbb{N}$, we assume that a_n is divisible by 9. We will show that a_{n+1} is divisible by 9. Since a_n is divisible by 9, there exists $j \in \mathbb{Z}$ such that $a_n = 9j$. Now, observe

$$a_{n+1} = 10^{n+1} - 1 = (9+1)10^n - 1 = 9 \cdot 10^n + 10^n - 1 = 9 \cdot 10^n + a_n = 9(10^n + j)$$

Since $10^n + j \in \mathbb{Z}$, we conclude that a_{n+1} is divisible by 9. Since the inductive step has been completed, the assertion is proven. $\square$

11.3. **Problem 3.** We show: $\forall\, n \in \mathbb{N}$, $2^n > n$.

Proof. We prove this assertion by induction on n. For $n = 1$ we have $2^1 = 2 > 1$, so the base case has been verified. We now proceed to the inductive step. For fixed $n \in \mathbb{N}$, assume that $2^n > n$. We will show that $2^{n+1} > n + 1$. Since $n \in \mathbb{N}$, $n \geq 1$, so $n + n \geq 1 + n$. From the given, $2^n > n$. Since 2^n and n are positive, $2 \cdot 2^n > 2n$. Since $2n \geq 1 + n$, we conclude that $2^{n+1} > n + 1$. Since the inductive step has been completed, the assertion is proven. $\square$

11.4. **Problem 4.** For $n \in \mathbb{N}$, let a_n be a sequence such that $a_1 = 3$, $a_2 = 3^2$, $a_3 = 3^3$, and $a_4 = 3^4$.

11.4.1. We explain what the value of a_5 could be.
From the information we have, a_5 could be any real number. It could be 0, π, $-1/2$, 3^5, etc. We cannot know what a_5 is since it has not been specified.

11.4.2. We find one rule that the sequence $a_n, n \in \mathbb{N}$ satisfies.
It could be that $a_n = 3^n$. In this case, $a_5 = 3^5 = 243$.

11.4.3. We find another rule for the sequence $a_n, n \in \mathbb{N}$.
It could be that $a_n = (n-1)(n-2)(n-3)(n-4) + 3^n$. In this case, $a_5 = 24 + 3^5 = 267$.

11.4.4. We explain whether or not the sequence $a_n, n \in \mathbb{N}$ is well defined.
The sequence $a_n, n \in \mathbb{N}$ is not well defined. We found two rules that satisfy our given information, and these rules give different values for a_5. Therefore, the sequence is not well defined.

12. Practice Final

12.1. **Problem 1.** We show that $|x-1| + |x+5| \geq 6$, $\forall\, x \in \mathbb{R}$.

Proof. We consider three separate cases, which cover all possible scenarios for the location of $x \in \mathbb{R}$. Case 1, $x < -5$. Case 2, $-5 \leq x \leq 1$. Case 3, $x > 1$.

Case 1, $x < -5$. In this case, $x - 1 < 0$ and $x + 5 < 0$, so $|x-1| + |x+5| = -(x-1) - (x+5) = -2x - 4$. Since $x < -5$, $-2x > 10$. Putting things together, we have $|x-1| + |x+5| > 10 - 4 = 6$, as desired.

Case 2, $-5 \leq x \leq 1$. In this case, $x - 1 \leq 0$ and $x + 5 \geq 0$, so $|x-1| + |x+5| = -(x-1) + (x+5) = 6$. In particular, $|x-1| + |x+5| \geq 6$, as desired.

Case 3, $x > 1$. In this case, $x-1>0$ and $x+5>0$, so $|x-1|+|x+5| = x-1+x+5 = 2x+4$. Since $x>1$, $2x>2$. Putting things together, we have $|x-1|+|x+5| > 2+4 = 6$, as desired.

In each case, we have shown that $|x-1|+|x+5| \geq 6$. Since these cases cover all possibilities for $x \in \mathbb{R}$, we conclude that $|x-1|+|x+5| \geq 6$, $\forall\, x \in \mathbb{R}$. $\square$

12.2. **Problem 2.** For $n \in \mathbb{N}$, $n \geq 3$, we show that $5^n + 6^n < 7^n$.

Proof. We prove the assertion by induction on n. We begin with the base case. Let $n=3$. Then $5^n + 6^n = 125 + 216 = 341 < 343 = 7^n$. With the base case verified, we now move on to the inductive step. Suppose for fixed $n \in \mathbb{N}$ that $5^n + 6^n < 7^n$. We prove as a result that $5^{n+1} + 6^{n+1} < 7^{n+1}$. Multiplying both sides of the given by 7, we have $7 \cdot 5^n + 7 \cdot 6^n < 7^{n+1}$. Since $5 < 7$ and $6 < 7$, we have $5 \cdot 5^n < 7 \cdot 5^n$ and $6 \cdot 6^n < 7 \cdot 6^n$. Combining our inequalities, we get $5^{n+1} + 6^{n+1} < 7^{n+1}$. With the inductive step completed, the desired assertion has been proven. $\square$

12.3. **Problem 3.** Consider the following statement: "If c is less than 20, then the equation $x^2 + 8x + c = 0$ has 2 real roots."

(i) We give an example that satisfies the statement.
(ii) We give an example that contradicts the statement.

(i) Let $c = 7$. Then $x^2 + 8x + 7 = (x+1)(x+7)$, so that the equation $x^2 + 8x + c = 0$ has two real roots, $x = -1$ and $x = -7$.

(ii) Let $c = 17$. Then $x^2 + 8x + 17 = (x+4-i)(x+4+i)$, where $i = \sqrt{-1}$. So, the equation $x^2 + 8x + c = 0$ has two roots that are not in $\mathbb{R}$.

12.4. **Problem 4.** We disprove the following statement: "For every $n \in \mathbb{N}$, $(3n^2 + 3n + 23)$ is a prime number."

Proof. Let $n = 23$. Then $3n^2 + 3n + 23 = 23(3n + 3 + 1)$. Since $n \in \mathbb{N}$, $3n + 3 + 1 \in \mathbb{Z}$, so 23 divides $3n^2 + 3n + 23$. That is, for $n = 23$, $3n^2 + 3n + 23$ is not a prime number. $\square$

12.5. **Problem 5.** Consider the following statement denoted by $(*)$.

$(*)$ For every $n \in \mathbb{N}$, $1 + 2 + 3 + \cdots + n = (n^2 + n + 2)/2$.

We study the following proof and answer the subsequent questions.

It is given that $(*)$ is true for $n = k$, $k \in \mathbb{N}$, that is, $1 + 2 + 3 + \cdots + k = (k^2 + k + 2)/2$. We will prove that $(*)$ is true for $n = k + 1$.

Proof.

$$\begin{aligned} 1 + 2 + 3 + \cdots + k + (k+1) &= \frac{k^2 + k + 2}{2} + (k+1) \qquad \text{, from the given information} \\ &= \frac{k^2 + k + 2 + 2(k+1)}{2} = \frac{k^2 + 3k + 3}{2} = \frac{(k+1)^2 + (k+1) + 2}{2} \end{aligned}$$

$\square$

(i) We believe (d) that the proof does not show anything about the truth-value of $(*)$.

(ii) The above proof is an incomplete inductive argument. We verified the inductive step, but we neglected to check the base case. Indeed, for $n = 1$, statement $(*)$ says that $1 = 2$, which is clearly false. So, we only showed that, if $(*)$ holds for $n \in \mathbb{N}$, then $(*)$ holds for $n+1$. However, $(*)$ is false for all $n \in \mathbb{N}$, since $1+2+\cdots+n = (n^2+n)/2$. Therefore, even though the implication in the above proof was a true implication, its hypothesis was false, so we have only proven a vacuous statement.

12.6. **Problem 6.** Consider the following statement: "For every $y \in \mathbb{Z}$, there exists $x \in \mathbb{Z}$ such that $x^2 = y$." We determine whether or not the given numbers below constitute a counterexample to the given statement.

(a) $y = 4$
(b) $y = .25$
(c) $y = -9$
(d) $y = -.16$

(a) Let $x = 2$. Then for $y = 4$, we have $x^2 = y$, so the statement is satisfied. Therefore, $y = 4$ is not a counterexample.

(b) For $y = .25$, $y \notin \mathbb{Z}$. Since the hypothesis of the statement is not satisfied, $y = .25$ is not a counterexample.

(c) Let $x \in \mathbb{Z}$. Then $x^2 \geq 0$. Since $y = -9$ satisfies $y < 0$, it is impossible to find $x \in \mathbb{Z}$ such that $x^2 = -9$. Since $y = -9$ satisfies the hypothesis of the statement, but it does not satisfy the conclusion of the statement, $y = -9$ is a counterexample.

(d) For $y = -.16$, $y \notin \mathbb{Z}$. Since the hypothesis of the statement is not satisfied, $y = -.16$ is not a counterexample.

12.7. **Problem 7.**

(a) We prove that the product of any 4 consecutive integers is always a multiple of 4.
(b) Let $x \in \mathbb{Z}$. We prove that, if $(x-1)(x+1)(x+2)$ is not divisible by 4, then x is divisible by 4.

Proof. (of (a)) Suppose our four consecutive integers are $x, y, z, a \in \mathbb{Z}$. Suppose we have also ordered these integers in ascending order, so that $x < y < z < a$. Since the integers are consecutive, $y = x+1, z = x+2$, and $a = x+3$. That is, our four consecutive integers are $x, x+1, x+2$ and $x+3$. By the Euclidean division algorithm, there exists $k, j \in \mathbb{Z}$ with $0 \leq j \leq 3$ such that $x = 4k + j$. We now consider all four cases of j separately. If $j = 0$, then $x = 4k$, so x is divisible by 4. If $j = 1$, then $x + 3 = 4k + 4 = 4(k+1)$, so $x+3$ is divisible by 4. If $j = 2$, then $x + 2 = 4k + 4 = 4(k+1)$, so $x + 2$ is divisible by 4. And if $j = 3$, then $x + 1 = 4k + 4 = 4(k+1)$, so $x + 1$ is divisible by 4.

We have shown that, among four consecutive integers, at least one of these integers is divisible by 4. As a result, the product $x(x+1)(x+2)(x+3)$ must also be divisible by 4, as desired. □

Proof. (of (b)) Observe that $x-1, x, x+1$ and $x+2$ are four consecutive integers. By our proof of part (a), at least one of these integers is divisible by 4. By assumption, $(x-1)(x+1)(x+2)$ is not divisible by 4. That is, $x-1, x+1$ and $x+2$ are each not divisible by 4, by the

Fundamental Theorem of Arithmetic. Since at least one of $x-1, x, x+1, x+2$ is divisible by 4, we must conclude that x is divisible by 4, as desired. $\square$

12.8. **Problem 8.** We show: $\forall\, n \in \mathbb{N}$, $4^n + 15n - 1$ is divisible by 9.

Proof. We prove the assertion by induction on n. We begin with the base case. For $n = 1$, we have $4^n + 15n - 1 = 18 = 2 \cdot 9$, so that the base case has been verified. We now begin with the inductive step. Assume that, for fixed $n \in \mathbb{N}$, $4^n + 15n - 1$ is divisible by 9. We will show that $4^{n+1} + 15(n+1) - 1$ is divisible by 9. From the given information, let $j \in \mathbb{Z}$ so that $4^n + 15n - 1 = 9j$. Then $4(4^n + 15n - 1) = 9(4j)$, i.e. $4^{n+1} + 15n + 45n - 4 + 14 - 14 = 9(4j)$, i.e. $4^{n+1} + 15(n+1) - 1 = 9(4j - 5n + 2)$. Since $j, n \in \mathbb{Z}$, $4j - 5n + 2 \in \mathbb{Z}$. We conclude that $4^{n+1} + 15(n+1) - 1$ is divisible by 9, as desired. $\square$

12.9. **Problem 9.** We prove that $\sqrt{5}$ is an irrational number.
See Problem 4.4(c).

13. Appendix: Notation

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}, \text{the set of integers}$$
$$\mathbb{N} = \{1, 2, 3, 4, 5, \ldots\}, \text{the set of natural numbers}$$
$$\mathbb{Q} = \{\ldots, 1/2, -2/3, 0, \ldots\} = \{m/n \colon m, n \in \mathbb{Z}, n \neq 0\}, \text{the set of rational numbers}$$
$$\mathbb{R} = \{\ldots, 1/2, \pi, \sqrt{3}, -.24534, -1, 4, 7.2, \ldots\}, \text{the set of real numbers}$$
$$\emptyset \text{ denotes the empty set, the set consisting of zero elements}$$
$$\in \text{ means “is an element of.” For example, } 2 \in \mathbb{Z} \text{ is read as “2 is an element of } \mathbb{Z}\text{.”}$$
$$\forall \text{ means “for all”}$$
$$\exists \text{ means “there exists”}$$

Remark 13.1. The symbol $\Rightarrow$ is not interchangeable with an equals sign.

Providing a rigorous definition of the real numbers is actually a bit of a challenge. It suffices to define $\mathbb{R}$ as the set of infinite decimals of the form $r = s \cdot b_n b_{n-1} \cdots b_0.a_1 a_2 a_3 a_4 \cdots$, where $n \in \mathbb{Z}$, $n \geq 0$, $s \in \{-1, 1\}$, for all $i \in \mathbb{Z}$, $a_i \in \mathbb{Z}$, $0 \leq a_i \leq 9$, for all $i \in \{1, 2, \ldots, n\}$, $b_i \in \mathbb{Z}$, $1 \leq b_i \leq 9$, $b_0 \in \mathbb{Z}$, $0 \leq b_0 \leq 9$, and such that the following does not occur: there exists $N \in \mathbb{N}, N > 0$ such that, for all $j > N$, $a_j = 9$. That is, we do not allow a constant, infinite sequence of 9's. Since we want the real numbers to be uniquely represented as infinite decimals, the fact that $0.9999999\ldots$ and 1 represent the same number is not desirable, so we eliminate one of these two representatives.