Section 6: Solutions

Proof by Contrapositve

1. Even Numbers, Odd Results!

(This question was also in Section 4)
For any integer j, if $3j + 1$ is even, then j is odd

(a) Write the predicate logic of this claim

Odd(x) := x is $2k + 1$, for some integer k
Even(x) := x is $2k$, for some integer k
Solution:

> $\forall j(Even(\text{3j+1}) \rightarrow Odd(\text{j}))$

(b) Write the contrapositive of this claim
Solution:

> For any integer j, if j is even, 3k+1 is odd
> $\forall \text{j}(Even(\text{j}) \rightarrow Odd(\text{3j+1}))$

(c) Prove this claim using a proof by contrapositive. **Solution:**

> **We will prove the contrapositive of this claim**
> Let j be an arbitrary even integer.
> By the definition of even $j = 2k$ for some integer k
> Then by Algebra, $3j + 1 = 3(2k) + 1 = 2(3k) + 1$
> Since k is an integer, under closure of multiplication, $3k$ is an integer
> Therefore 2(3k) + 1 takes the form of an odd integer so $3j + 1$ must be odd Since j was arbitrary and we have shown the contrapositive, the claim holds

2. The Trifecta

(This question was also in Section 4)
Consider the following proposition: For each integer a, if 3 divides a^2, then 3 divides a

(a) Write the contrapositive of this proposition as a sentence:
Solution:

> For any integer a, if 3 does not divide a then 3 does not divide a^2

(b) Prove the proposition by proving its contrapositive.
Hint: Consider using cases based on the remainder for "division by 3." There will be two cases! **Solution:**

We will prove the contrapositive of this claim
Let a be an arbitrary integer. Suppose that 3 does not divide a. By the division theorem, there must be an integer $0 \leq r < 3$ and an integer k such that $a = 3k + r$. Since r can't be 0 (no integer k such that $a = 3k$ by definition of divides), the remainder r is either 1 or 2.

Case 1: $r = 1$
a can be expressed as an integer with remainder 1 as, $a = 3k + 1, k \in \mathbb{Z}$
Similarly, we define a^2 as $a \cdot a = (3k+1) \cdot (3k+1) = 9k^2 + 6k + 1 = 3(3k^2 + 2k) + 1$. $3k^2 + 2k$ is an integer under closure of addition and multiplication, but then we've written a^2 as $3j + 1$ for some integer j. By the division theorem, 1 is the unique integer that can appear as z in the expression $a^2 = 3w + z$, where z is an integer between 0 and 2 and w is an integer. Thus 3 cannot divide a^2, as if 3 does divide a^2, we would have a formula with $z = 0$.

Case 2: $r = 2$
a can be expressed as an integer with remainder 2 as $a = 3k + 2, k \in \mathbb{Z}$
Similarly, we define a^2 as $a \cdot a = (3k+2) \cdot (3k+2) = 9k^2 + 12k + 4 = 9k^2 + 12k + 3 + 1 = 3(3k^2 + 4k + 1) + 1$. $3k^2 + 4k + 1$ is an integer under closure of addition and multiplication, but then we have written a^2 as $3j + 2$ for some integer j. By the division theorem, 2 is the unique integer that can appear as z in the expression $a^2 = 3w + z$, where z is an integer between 0 and 2 and w is an integer. Thus 3 cannot divide a^2, as if 3 does divide a^2, we would have a formula with $z = 0$.

In both cases, we have that 3 does not divide a^2. Since a was arbitrary, and we have demonstrated the contrapositive, the claim holds

Proof by Contradiction

3. Wait, That Doesn't Add Up

(This question was also in Section 5)
Write a proof by contradiction for the following proposition: There exist no integers x and y such that $18x + 6y = 1$.
HINT: Try writing in propositional logic, then negating this statement before writing your proof.

Solution:

In predicate logic this could be expressed as $\forall x \forall y (18x + 6y \neq 1)$.

Assume, for the sake of contradiction, that there exists integers x and y such that $18x + 6y = 1$. This gives us:

$$\begin{aligned} 18x + 6y &= 1 \\ 3x + y &= \frac{1}{6} && \text{Dividing by 6} \end{aligned}$$

But wait, this is a contradiction! Integers are closed under multiplication and addition, and so $3x + y$ can't be equal to $\frac{1}{6}$. This means there can be no integers x and y such that $18x + 6y = 1$. Therefore, the original claim holds via proof by contradiction.

4. Prime Checking

This question is part of a question on the Section 5 handout - take a look at the handout for the full context and question.
We will use "nontrivial divisor" to mean a factor that isn't 1 or the number itself. Formally, a positive integer k being a "nontrivial divisor" of n means that $k|n$, $k \neq 1$ and $k \neq n$.
Claim: For every positive integer n, if n has a nontrivial divisor, then it has a nontrivial divisor at most $\sqrt{n}$.

Prove the claim. Hint: we recommend a proof by contradiction.

Solution:

Proof by Contradiction:
Before we begin the actual proof, let's write the claim in propositional logic and negate it: Let $D(n,k)$ be true iff k is a nontrivial divisor of n. This claim in predicate logic is $\forall n(\exists k(D(n,k)) \rightarrow \exists k(D(n,k) \wedge k \leq \sqrt{n}))$. The negation of this is $\exists n[\exists k(D(n,k)) \wedge \forall k(D(n,k) \rightarrow (k > \sqrt{n}))]$

We start by supposing the negation of the claim is true: Suppose, for the sake of contradiction, that there is an n such that n has a non-trivial divisor and all its nontrivial divisors are greater than $\sqrt{n}$.

Let k be a nontrivial divisor of n. Since k is a divisor, $n = kc$ for some integer c. Observe that c is also is divisor $c|n$ since there is a integer k such that $n = ck$. c is also nontrivial, since we know that k is not n nor 1 by def. of nontrivial, and if c were 1 or n then k would have to be n or 1.

Since both k and n are non-trivial divisors, we have that $k > \sqrt{n}$ and $c > \sqrt{n}$. Then $kc > \sqrt{n}\sqrt{n} = n$. But by assumption we have $kc = n$, so this is a contradiction. Thus we conclude our original claim—that if a positive integer n has a nontrivial divisor, then it has a nontrivial divisor at most $\sqrt{n}$—is true.

Alternative proof by cases:
Let k be a nontrivial divisor of n. Since k is a divisor, $n = kc$ for some integer c. Observe that c is also nontrivial, since if c were 1 or n then k would have to be n or 1.

We now have two cases:

Case 1: $k \leq \sqrt{n}$
If $k \leq \sqrt{n}$, then we're done because k is the desired nontrivial divisor.

Case 2: $k > \sqrt{n}$
If $k > \sqrt{n}$, then multiplying both sides by c we get $ck > c\sqrt{n}$. But $ck = n$ so $n > c\sqrt{n}$. Finally, dividing both sides by $\sqrt{n}$ gives $\sqrt{n} > c$, so c is the desired nontrivial factor.

In both cases we find a nontrivial divisor at most $\sqrt{n}$, as required.

A Set of Set Questions

5. How Many Elements?

For each of these, how many elements are in the set? If the set has infinitely many elements, say ∞.

(a) $A = \{1, 2, 3, 2\}$

Solution:

3

(b) $B = \{\emptyset,\ \{\emptyset\},\ \{\emptyset, \emptyset\},\ \{\emptyset, \emptyset, \emptyset\},\ \ldots\}$

Solution:

$$\begin{aligned} B &= \{\emptyset,\ \{\emptyset\},\ \{\emptyset, \emptyset\},\ \{\emptyset, \emptyset, \emptyset\},\ \ldots\} \\ &= \{\{\},\ \{\{\}\},\ \{\{\}\},\ \{\{\}\},\ \ldots\} \\ &= \{\emptyset, \{\emptyset\}\} \end{aligned}$$

So, there are two elements in B.

(c) $C = A \times (B \cup \{7\})$

Solution:

$C = \{1, 2, 3\} \times \{\emptyset, \{\emptyset\}, 7\} = \{(a, b) \mid a \in \{1, 2, 3\}, b \in \{\emptyset, \{\emptyset\}, 7\}\}$. It follows that there are $3 \times 3 = 9$ elements in C.

(d) $D = \emptyset$

Solution:

0.

(e) $E = \{\emptyset\}$

Solution:

1.

(f) $F = \mathcal{P}(\{\emptyset\})$

Solution:

$2^1 = 2$. The elements are $F = \{\emptyset, \{\emptyset\}\}$.

6. Just The Setup

For this statement,

- Translate the sentence into predicate logic.
- Write the first few sentences and last few sentences of the English proof.

If $A \subseteq B$ and $B \subseteq C$, then $A \subseteq C$ for any sets A, B, C.

Solution:

$(A \subseteq B \wedge B \subseteq C) \rightarrow A \subseteq C$

Let A, B, C be arbitrary sets.
Suppose $A \subseteq B$ and $B \subseteq C$.
Let a be an arbitrary element of A.
...
Included here for completenes...
By definition of subset, $a \in B$. Applying definition of subset again since $B \subseteq C$, $a \in C$. Thus, since we found for an arbitrary element a if $a \in A$, then $a \in C$, by definition of subset, $A \subseteq C$.

Hence, a is an element of C.
Since a was arbitrary, every element of A is an element of C, so $A \subseteq C$.

7. Set Theory

Suppose that $A \subseteq B$. Prove that $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

Solution:

Suppose $A \subseteq B$. Let $X \in \mathcal{P}(A)$ be an arbitrary element. Then by definition of powerset, $X \subseteq A$. Let $y \in X$ be arbitrary. Then since $X \subseteq A$, by definition of subset, $y \in A$. Since $A \subseteq B$, by definition of subset again, $y \in B$. Since y was arbitrary in X, by definition of subset once more, $X \subseteq B$. Then by definition of powerset, $X \in \mathcal{P}(B)$. Since X was arbitrary in $\mathcal{P}(A)$, we have shown $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

8. Set = Set

Prove the following set identities. Write an English proof.

(a) Let the universal set be $\mathcal{U}$. Prove $A \cap \overline{B} \subseteq A \setminus B$ for any sets A, B.

Solution:

Let x be an arbitrary element and suppose that $x \in A \cap \overline{B}$. By definition of intersection, $x \in A$ and $x \in \overline{B}$, so by definition of complement, $x \notin B$. Then, by definition of set difference, $x \in A \setminus B$. Since x was arbitrary, we can conclude that $A \cap \overline{B} \subseteq A \setminus B$ by definition of subset.

(b) Prove that $(A \cap B) \times C \subseteq A \times (C \cup D)$ for any sets A, B, C, D.

Solution:

Let x be an arbitrary element of $(A \cap B) \times C$. Then, by definition of Cartesian product, x must be of the form (y, z) where $y \in A \cap B$ and $z \in C$. Since $y \in A \cap B$, $y \in A$ and $y \in B$ by definition of $\cap$; in particular, all we care about is that $y \in A$. Since $z \in C$, by definition of $\cup$, we also have $z \in C \cup D$. Therefore since $y \in A$ and $z \in C \cup D$, by definition of Cartesian product we have $x = (y, z) \in A \times (C \cup D)$.

Since x was an arbitrary element of $(A \cap B) \times C$ we have proved that $(A \cap B) \times C \subseteq A \times (C \cup D)$ as required.

9. Set Equality

Prove that $A \cap (A \cup B) = A$ for any sets A, B.

Solution:

Let x be an arbitrary member of $A \cap (A \cup B)$. Then by definition of intersection, $x \in A$ and $x \in A \cup B$. So certainly, $x \in A$. Since x was arbitrary, $A \cap (A \cup B) \subseteq A$.

Now let y be an arbitrary member of A. Then $y \in A$. So certainly $y \in A$ or $y \in B$. Then by definition of union, $y \in A \cup B$. Since $y \in A$ and $y \in A \cup B$, by definition of intersection, $y \in A \cap (A \cup B)$. Since y was arbitrary, $A \subseteq A \cap (A \cup B)$.

Therefore $A \cap (A \cup B) = A$, by containment in both directions.

Intro to Induction

10. Induction with Equality

(a) Show using induction that $0+1+2+\cdots+n=\frac{n(n+1)}{2}$ for all $n\in\mathbb{N}$.

Solution:

For $n\in\mathbb{N}$ let $P(n)$ be "$0+1+\cdots+n=\frac{n(n+1)}{2}$". We show $P(n)$ for all $n\in\mathbb{N}$ by induction on n.

Base Case: We have $0=0=\frac{0(0+1)}{2}$ which is $P(0)$ so the base case holds.

Inductive Hypothesis: Suppose $P(k)$ holds for some arbitrary integer $k\geq 0$.

Inductive Step: $\boxed{\text{Goal: Show } 0+1+\cdots+(k+1)=\dfrac{(k+1)(k+2)}{2}}$.

We have

$$\begin{aligned}
0+1+\cdots+k+(k+1) &= (0+1+\cdots+k)+(k+1) \\
&= \frac{k(k+1)}{2}+(k+1) && \text{[Inductive Hypothesis]} \\
&= \frac{k(k+1)}{2}+\frac{2(k+1)}{2} \\
&= \frac{k(k+1)+2(k+1)}{2} \\
&= \frac{(k+1)(k+2)}{2} && \text{[Factor out } (k+1)\text{]}
\end{aligned}$$

This proves $P(k+1)$.

Conclusion: $P(n)$ holds for all $n\in\mathbb{N}$ by the principle of induction.

(b) Define the triangle numbers as $\triangle_n=1+2+\cdots+n$, where $n\in\mathbb{N}$. In part (a) we showed $\triangle_n=\frac{n(n+1)}{2}$. Prove the following equality for all $n\in\mathbb{N}$:

$$0^3+1^3+\cdots+n^3=\triangle_n^2$$

Solution:

First, note that $\triangle_n=(0+1+2+\cdots+n)$. So, we are trying to prove $(0^3+1^3+\cdots+n^3)=(0+1+\cdots+n)^2$. Let $P(n)$ be the statement:

$$0^3+1^3+\cdots+n^3=(0+1+\cdots+n)^2.$$

We prove that $P(n)$ is true for all $n\in\mathbb{N}$ by induction on n.

Base Case. $0^3=0=0^2$, so $P(0)$ holds.

Inductive Hypothesis. Suppose that $P(k)$ is true for some arbitrary $k\in\mathbb{N}$.

Inductive Step. We show $P(k+1)$:

$$\begin{aligned}
0^3 + 1^3 + \cdots (k+1)^3 &= (0^3 + 1^3 + \cdots + k^3) + (k+1)^3 && \text{[Associativity7]} \\
&= (0 + 1 + \cdots + k)^2 + (k+1)^3 && \text{[Inductive Hypothesis]} \\
&= \left(\frac{k(k+1)}{2}\right)^2 + (k+1)^3 && \text{[Part (a)]} \\
&= (k+1)^2 \left(\frac{k^2}{2^2} + (k+1)\right) && \text{[Factor } (k+1)^2\text{]} \\
&= (k+1)^2 \left(\frac{k^2 + 4k + 4}{4}\right) && \text{[Add via common denominator]} \\
&= (k+1)^2 \left(\frac{(k+2)^2}{4}\right) && \text{[Factor numerator]} \\
&= \left(\frac{(k+1)(k+2)}{2}\right)^2 && \text{[Take out the square]} \\
&= (0 + 1 + \cdots + (k+1))^2 && \text{[Part (a)]}
\end{aligned}$$

Conclusion: $P(n)$ is true for all $n \in \mathbb{N}$ by the principle of induction.

11. Induction with Divides

Prove that $9 \mid (n^3 + (n+1)^3 + (n+2)^3)$ for all $n > 1$ by induction. **Solution:**

Let $P(n)$ be "$9 \mid n^3 + (n+1)^3 + (n+2)^3$". We will prove $P(n)$ for all integers $n > 1$ by induction.

Base Case $(n = 2)$**:** $2^3 + (2+1)^3 + (2+2)^3 = 8 + 27 + 64 = 99 = 9 \cdot 11$, so $9 \mid 2^3 + (2+1)^3 + (2+2)^3$, so $P(2)$ holds.

Induction Hypothesis: Assume that $9 \mid j^3 + (j+1)^3 + (j+2)^3$ for an arbitrary integer $j > 1$. Note that this is equivalent to assuming that $j^3 + (j+1)^3 + (j+2)^3 = 9k$ for some integer k by the definition of divides.

Induction Step: Goal: Show $9 \mid (j+1)^3 + (j+2)^3 + (j+3)^3$

$$\begin{aligned}
(j+1)^3 + (j+2)^3 + (j+3)^3 &= (j+3)^3 + 9k - j^3 \text{ for some integer } k && \text{[Induction Hypothesis]} \\
&= j^3 + 9j^2 + 27j + 27 + 9k - j^3 \\
&= 9j^2 + 27j + 27 + 9k \\
&= 9(j^2 + 3j + 3 + k)
\end{aligned}$$

Since j is an integer, $j^2 + 3j + 3 + k$ is also an integer. Therefore, by the definition of divides, $9 \mid (j+1)^3 + (j+2)^3 + (j+3)^3$, so $P(j) \to P(j+1)$ for an arbitrary integer $j > 1$.

Conclusion: $P(n)$ holds for all integers $n > 1$ by induction.

12. Induction with Inequality

Prove that $6n + 6 < 2^n$ for all $n \geq 6$. **Solution:**

Let $P(n)$ be "$6n + 6 < 2^n$". We will prove $P(n)$ for all integers $n \geq 6$ by induction on n

Base Case $(n = 6)$**:** $6 \cdot 6 + 6 = 42 < 64 = 2^6$, so $P(6)$ holds.

Inductive Hypothesis: Assume that $6k + 6 < 2^k$ for an arbitrary integer $k \geq 6$.

Inductive Step: Goal: Show $6(k+1)+6 < 2^{k+1}$

$$\begin{aligned}
6(k+1)+6 &= 6k+6+6 \\
&< 2^k + 6 && \text{[Inductive Hypothesis]} \\
&< 2^k + 2^k && \text{[Since } 2^k > 6\text{, since } k \geq 6\text{]} \\
&= 2 \cdot 2^k \\
&= 2^{k+1}
\end{aligned}$$

So $P(k) \to P(k+1)$ for an arbitrary integer $k \geq 6$.

Conclusion: $P(n)$ holds for all integers $n \geq 6$ by the principle of induction.