# Section MR: Solutions

## 1. Midterm Review: English Proof (Even Steven)

Prove that for all integers k, k(k +3) is even.
Recall that $\texttt{Even}(x) := \exists k(x = 2k)$ and $\texttt{Odd}(x) := \exists k(x = 2k + 1)$

(a) Let your domain be integers. Write this claim in predicate logic.

**Solution:**

$\forall k(Even(k(k + 3)))$

(b) Write an English proof for this claim. **Solution:**

Let $k$ be an arbitrary integer.
**Case 1: $k$ is even**
By the definition of even, $k = 2j$ for some integer $j$
So substituting for $k$ into $k(k + 3)$:

$$k(k + 3) = (2j)(2j + 3) = 2(2j^2 + 3j)$$

$k(k + 3) = 2n$, where $n = (2j^2 + 3j)$ and $n$ is an integer since $j$ is an integer and integers are closed under addition and multiplication.
So, by definition of even, $k(k + 3)$ is even.

**Case 2: $k$ is odd**
By the definition of odd, $k = 2j + 1$ for some integer $j$.
So substituting for $k$ into k(k+3):

$$k(k + 3) = (2j + 1)(2j + 1 + 3) = (2j + 1)(2j + 4) = 4j^2 + 10j + 4 = 2(2j^2 + 5j + 2) = 2(2j + 1)(j + 2)$$

$k(k + 3) = 2n$, where $n = (2j + 1)(j + 2)$ and $n$ is an integer since $j$ is an integer and integers are closed under addition and multiplication.
So, by definition of even, $k(k + 3)$ is even.

**These cases are exhaustive, so the claim that $k(k + 3)$ is even must hold.**
Since $k$ was arbitrary, the claim holds for all $k$.

## 2. Midterm Review: Proof by Contradiction

*(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:

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

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.

## 3. Midterm Review: Number Theory

Let $p$ be a prime number at least 3, and let $x$ be an integer such that $x^2 \% p = 1$.

(a) Show that if an integer $y$ satisfies $y \equiv 1 \pmod{p}$, then $y^2 \equiv 1 \pmod{p}$. (this proof will be short!)
(Try to do this without using the theorem "Raising Congruences To A Power")
**Solution:**

Let $y$ be an arbitrary integer and suppose $y \equiv 1 \pmod{p}$. We can multiply congruences, so multiplying this congruence by itself we get $y^2 \equiv 1^2 \pmod{p}$. Since $y$ is arbitrary, the claim holds.

(b) Repeat part (a), but don't use any theorems from the Number Theory Reference Sheet. That is, show the claim directly from the definitions. **Solution:**

Let $x$ be an arbitrary integer and suppose $x \equiv 1 \pmod{p}$. By the definition of Congruences, $p \mid (x - 1)$. Therefore, by the definition of divides, there exists an integer $k$ such that

$$pk = (x - 1)$$

By multiplying both sides of pk = (x - 1) by (x + 1) and re-arranging the equation, we have

$$\begin{aligned} pk(x+1) &= (x-1)(x+1) \\ p(k(x+1)) &= (x-1)(x+1) \end{aligned}$$

Since $(x-1)(x+1) = x^2 - 1$, by replacing $(x-1)(x+1)$ with $x^2 - 1$, we have

$$p(k(x+1)) = x^2 - 1$$

Note that since $k$ and $x$ are integers, (k (x + 1)) is also an integer. Therefore, by the definition of divides $p \mid x^2 - 1$.
Hence, by the definition of Congruences, $x^2 \equiv 1 \pmod{p}$.

(c) From part (a), we can see that $x\%p$ can equal 1. Show that for any integer $x$, if $x^2 \equiv 1 \pmod{p}$, then $x \equiv 1 \pmod{p}$ or $x \equiv -1 \pmod{p}$. That is, show that the only value $x\%p$ can take other than 1 is $p - 1$.
Hint: Suppose you have an $x$ such that $x^2 \equiv 1 \pmod{p}$ and use the fact that $x^2 - 1 = (x-1)(x+1)$
Hint: You may the following theorem without proof: if $p$ is prime and $p \mid (ab)$ then $p \mid a$ or $p \mid b$. **Solution:**

Let $x$ be an arbitrary integer and suppose $x^2 \equiv 1 \pmod{p}$. By the definition of Congruences,

$$p \mid x^2 - 1$$

Since $(x-1)(x+1) = x^2 - 1$, by replacing $x^2 - 1$ with $(x-1)(x+1)$, we have

$$p \mid (x-1)(x+1)$$

Note that for an integer $p$ if $p$ is a prime number and $p \mid (ab)$, then $p \mid a$ or $p \mid b$. In this case, since $p$ is a prime number, by applying the rule, we have $p \mid (x-1)$ or $p \mid (x+1)$.
Therefore, by the definition of Congruences, we have $x \equiv 1 \pmod{p}$ or $x \equiv -1 \pmod{p}$.

## *Induction*

## 4. Midterm Review: Induction

For any $n \in \mathbb{N}$, define $S_n$ to be the sum of the squares of the first $n$ positive integers, or

$$S_n = 1^2 + 2^2 + \cdots + n^2.$$

Prove that for all $n \in \mathbb{N}$, $S_n = \frac{1}{6}n(n+1)(2n+1)$. **Solution:**

Let $\mathsf{P}(n)$ be the statement "$S_n = \frac{1}{6}n(n+1)(2n+1)$" defined for all $n \in \mathbb{N}$. We prove that $\mathsf{P}(n)$ is true for all $n \in \mathbb{N}$ by induction on $n$.

**Base Case:** When $n = 0$, we know the sum of the squares of the first $n$ positive integers is the sum of no terms, so we have a sum of 0. Thus, $S_0 = 0$. Since $\frac{1}{6}(0)(0+1)((2)(0)+1) = 0$, we know that $\mathsf{P}(0)$ is true.

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

**Inductive Step:** Examining $S_{k+1}$, we see that

$$S_{k+1} = 1^2 + 2^2 + \cdots + k^2 + (k+1)^2 = S_k + (k+1)^2.$$

By the inductive hypothesis, we know that $S_k = \frac{1}{6}k(k+1)(2k+1)$. Therefore, we can substitute and rewrite the expression as follows:

$$\begin{aligned}
S_{k+1} &= S_k + (k+1)^2 \\
&= \frac{1}{6}k(k+1)(2k+1) + (k+1)^2 \\
&= (k+1)\left(\frac{1}{6}k(2k+1) + (k+1)\right) \\
&= \frac{1}{6}(k+1)\left(k(2k+1) + 6(k+1)\right) \\
&= \frac{1}{6}(k+1)\left(2k^2 + 7k + 6\right) \\
&= \frac{1}{6}(k+1)(k+2)(2k+3) \\
&= \frac{1}{6}(k+1)((k+1)+1)(2(k+1)+1)
\end{aligned}$$

Thus, we can conclude that $\mathsf{P}(k+1)$ is true.

**Conclusion:** $P(n)$ holds for all integers $n \geq 0$ by the principle of induction.

## 5. Midterm Review: Strong Induction

Robbie is planning to buy snacks for the members of his competitive roller-skating troupe. However, his local grocery store sells snacks in packs of 5 and packs of 7.

Prove that Robbie can buy exactly $n$ snacks for all integers $n \geq 24$

**Solution:**

Let $\mathsf{P}(n)$ be the statement "Robbie can buy $n$ snacks with packs of 5 and packs of 7 snacks" defined for all $n \geq 24$. We prove that $\mathsf{P}(n)$ is true for all $n \geq 24$ by the principle of strong induction.

**Base Case:**

n = 24: 24 snacks can be bought with 2 packs of 7 and 2 packs of 5 snacks.
n = 25: 25 snacks can be bought with 5 packs of 5 snacks.
n = 26: 26 snacks can be bought with 3 packs of 7 and 1 pack of 5 snacks.
n = 27: 27 snacks can be bought with 1 pack of 7 and 4 packs of 5 snacks.
n = 28: 28 snacks can be bought with 4 packs of 7 snacks.

**Inductive Hypothesis:** Suppose that $\mathsf{P}(24) \wedge \mathsf{P}(25) \wedge \ldots \wedge \mathsf{P}(k)$ is true for some arbitrary $k \geq 28$.

**Inductive Step:** We want to show that Robbie can buy exactly $k+1$ snacks. By the inductive hypothesis, we know that Robbie can buy exactly $k-4$ snacks, so he can buy another pack of 5 to get exactly $k+1$ snacks.

**Conclusion:** Therefore, $\mathsf{P}(n)$ holds for all integers $n \geq 24$ by the principle of strong induction.

## 6. Midterm Review: Reversing a Binary Tree (Structural Induction)

Consider the following definition of a (binary) **Tree**.

**Basis Step** `Nil` is a **Tree**.

**Recursive Step** If $L$ is a **Tree**, $R$ is a **Tree**, and $x$ is an integer, then $\texttt{Tree}(x, L, R)$ is a **Tree**.

The $\mathsf{sum}$ function returns the sum of all elements in a **Tree**.

$$\begin{aligned} \mathsf{sum}(\texttt{Nil}) &= 0 \\ \mathsf{sum}(\texttt{Tree}(x, L, R)) &= x + \mathsf{sum}(L) + \mathsf{sum}(R) \end{aligned}$$

The following recursively defined function produces the mirror image of a **Tree**.

$$\begin{aligned} \mathsf{reverse}(\texttt{Nil}) &= \texttt{Nil} \\ \mathsf{reverse}(\texttt{Tree}(x, L, R)) &= \texttt{Tree}(x, \mathsf{reverse}(R), \mathsf{reverse}(L)) \end{aligned}$$

Show that, for all **Tree**s $T$ that

$$\mathsf{sum}(T) = \mathsf{sum}(\mathsf{reverse}(T))$$

**Solution:**

For a **Tree** $T$, let $P(T)$ be "$\mathsf{sum}(T) = \mathsf{sum}(\mathsf{reverse}(T))$". We show $P(T)$ for all **Tree**s $T$ by structural induction.

**Base Case:** By definition we have $\mathsf{reverse}(\texttt{Nil}) = \texttt{Nil}$. Applying $\mathsf{sum}$ to both sides we get $\mathsf{sum}(\texttt{Nil}) = \mathsf{sum}(\mathsf{reverse}(\texttt{Nil}))$, which is exactly $P(\texttt{Nil})$, so the base case holds.

**Inductive Hypothesis:** Suppose $P(L)$ and $P(R)$ hold for some arbitrary **Tree**s $L$ and $R$.

**Inductive Step:** Let $x$ be an arbitrary integer. Goal: Show $P(\texttt{Tree}(x, L, R))$ holds.

We have,

$$\begin{aligned}
\textsf{sum}(\textsf{reverse}(\texttt{Tree}(x, L, R))) &= \textsf{sum}(\texttt{Tree}(x, \textsf{reverse}(R), \textsf{reverse}(L))) && \text{[Definition of reverse]} \\
&= x + \textsf{sum}(\textsf{reverse}(R)) + \textsf{sum}(\textsf{reverse}(L)) && \text{[Definition of sum]} \\
&= x + \textsf{sum}(R) + \textsf{sum}(L) && \text{[Inductive Hypothesis]} \\
&= x + \textsf{sum}(L) + \textsf{sum}(R) && \text{[Commutativity]} \\
&= \textsf{sum}(\texttt{Tree}(x, L, R)) && \text{[Definition of sum]}
\end{aligned}$$

This shows $P(\texttt{Tree}(x, L, R))$.

**Conclusion:** Therefore, $P(T)$ holds for all **Tree**s $T$ by structural induction.

## *Set Theory*

## 7. Midterm Review: Unioned Intersections (Proof by [Counter]example)

Show that there exists sets $A, B, C, D, E, F$ such that $(A \cap B) \cup (C \cap D) \cup (E \cap F) \nsubseteq (A \cup B) \cap (C \cup D) \cap (E \cup F)$. *(In other words,* ***disprove*** *the claim, "for all sets,* $(A \cap B) \cup (C \cap D) \cup (E \cap F) \subseteq (A \cup B) \cap (C \cup D) \cap (E \cup F)$*).*

**Solution:**

Consider sets $A = B = \{3\}, C = D = E = F = \{5\}$.

$A \cap B$ is the set $\{3\}$, $C \cap D$ is the set $\{5\}$, and $E \cap F$ is the set $\{5\}$.
The union of these sets is $(A \cap B) \cup (C \cap D) \cup (E \cap F) = \{3, 5\}$.

$A \cup B$ is the set $\{3\}$, $C \cup D$ is the set $\{5\}$, and $E \cup F$ is the set $\{5\}$.
There are no elements that exist in all 3 of these sets, so the intersection $(A \cup B) \cap (C \cup D) \cap (E \cup F)$ is the empty set $\emptyset$.

Consider $x = 3$.
We can see that $x \in (A \cap B) \cup (C \cap D) \cup (E \cap F)$ but $x \notin (A \cup B) \cap (C \cup D) \cap (E \cup F)$.
So, it is not true that all elements in $(A \cap B) \cup (C \cap D) \cup (E \cap F)$ are in $(A \cup B) \cap (C \cup D) \cap (E \cup F)$.
By definition of subset, we have found sets $A, B, C, D, E, F$ such that $(A \cap B) \cup (C \cap D) \cup (E \cap F) \nsubseteq (A \cup B) \cap (C \cup D) \cap (E \cup F)$ which is exactly the claim we are trying to prove.

***Note***: There are many possible values of $x$ and sets that would give an example we're looking for (including cases where some of the sets are empty sets). All we need is to show some example that makes the claim true, so we only need (and should) give one example.

## 8. Midterm Review: Complementary Sets (Proof by Contrapositive)

We want to write a proof for $\overline{A \cup B} \subseteq \overline{A \cap B}$.

(a) Translate $\overline{A \cup B} \subseteq \overline{A \cap B}$ to predicate logic (it should contain an implication!). **Solution:**

$$\forall x(x \notin A \cup B \rightarrow x \notin A \cap B)$$

The definition of subset translates $\forall x(x \in \overline{A \cup B} \rightarrow x \in \overline{A \cap B})$. Applying the definition of complement gives $\forall x(x \notin A \cup B \rightarrow x \notin A \cap B)$.

(b) Take the contrapositive of the statement in (a). **Solution:**

$$\forall x(x \in A \cap B \rightarrow x \in A \cup B)$$

(c) Write the expression from (b) in set notation. **Solution:**

Applying the definition of subset, $A \cap B \subseteq A \cup B$.

(d) Write an English proof for the statement in part (c).
(Note: you are effectively doing a proof by contrapositive!) **Solution:**

We argue by contrapositive.
Let $x$ be an arbitrary element of $A \cap B$.
By definition of intersection, $x \in A$ and $x \in B$.
Since $x \in A$, then $x \in A$ or $x \in B$
Applying the definition of union, $x \in A \cup B$.
Since $x$ was an arbitrary element of $A \cap B$, we have shown that $A \cap B \subseteq A \cup B$.

## 9. Midterm Review: Power Crossing (Power Sets and Cartesian Products)

Show that $\mathcal{P}(A) \times \mathcal{P}(B) \subseteq \mathcal{P}(A \cup C) \times \mathcal{P}(B \cup C)$. **Solution:**

Let $x \in \mathcal{P}(A) \times \mathcal{P}(B)$ be arbitrary.
By definition of Cartesian product, there exist some elements $Y \in \mathcal{P}(A)$ and $Z \in \mathcal{P}(B)$ such that $x = (Y, Z)$.

Since $Y \in \mathcal{P}(A)$, by definition of powerset, $Y \subseteq A$.
Let $y \in Y$ be arbitrary.
Since $Y \subseteq A$, by definition of subset, $y \in A$.
Since $y \in A$, then $y \in A$ or $y \in C$.
Applying the definition of union, $y \in A \cup C$.
Since $y \in Y$ was arbitrary, applying the definition of subset, $Y \subseteq A \cup C$.
Applying the definition of powerset, $Y \in \mathcal{P}(A \cup C)$.

Since $Z \in \mathcal{P}(B)$, by definition of powerset, $Z \subseteq B$.
Let $z \in Z$ be arbitrary.
Since $Z \subseteq B$, by definition of subset, $z \in B$.
Since $z \in B$, then $z \in B$ or $z \in C$.
Applying the definition of union, $z \in B \cup C$.
Since $z \in Z$ was arbitrary, applying the definition of subset, $Z \subseteq B \cup C$.
Applying the definition of powerset, $Z \in \mathcal{P}(B \cup C)$.

Since $Y \in \mathcal{P}(A \cup C)$ and $Z \in \mathcal{P}(B \cup C)$, applying the definition of Cartesian product, $(Y, Z) \in \mathcal{P}(A \cup C) \times \mathcal{P}(B \cup C)$.
Since $x = (Y, Z)$ and $(Y, Z) \in \mathcal{P}(A \cup C) \times \mathcal{P}(B \cup C)$, $x \in \mathcal{P}(A \cup C) \times \mathcal{P}(B \cup C)$.
Since $x \in \mathcal{P}(A) \times \mathcal{P}(B)$ was arbitrary, applying the definition of subset, we have shown that $\mathcal{P}(A) \times \mathcal{P}(B) \subseteq \mathcal{P}(A \cup C) \times \mathcal{P}(B \cup C)$.