CSE 311 Section MR

Midterm Review

Administrivia

Announcements & Reminders

- HW5 grades released
  - Take a look at common errors posts for set and induction proofs!!
- HW6
  - Due Wednesday 11/12

- Midterm 2 is Coming Next Week!!!

General Tips!

General Tips

- Always **start with the template/start and end**!! Especially for induction, you will likely get partial credit if you have a correct filled in template
- After completing a proof, **read through it top to bottom** and make sure every step flows and follows from the previous
- It is often very helpful to "**work backwards**" from what you are trying to prove to plan your approach, but your **final written proof should still go forward logically**.
    - If you do work backwards while thinking, leave a clear gap and write those steps from the bottom up—then check that every step remains valid when you read the proof from top to bottom.
- Make sure you are **defining variables are arbitrary when appropriate** (it's not a magic word, only applies if anything we say about that variable will apply to *any* value), and **specify its type** (e.g., integer)

Problem 1: Even Steven

Problem 1: Even Steven

Prove that for all integers k, k(k +3) is even.

Recall that Even(x) := $\exists k(x = 2k)$ and Odd(x) := $\exists k(x = 2k + 1)$

Step 1. Write in predicate logic

Step 2. Prove it!

Problem 1: Even Steven

Great! Let's make a template, start and end for the proof...

Prove that for all integers k, k(k +3) is even.

Recall that Even(x) := $\exists k(x = 2k)$ and Odd(x) := $\exists k(x = 2k + 1)$

Step 1. Write in predicate logic

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

Step 2. Prove it!

Problem 1: Even Steven

Before we go on, what exactly are we trying to prove? Let's apply the def of even...

Prove that for all integers k, k(k +3) is even.

Predicate logic: $\forall k(Even(k(k + 3)))$

Step 2. Prove it!

Let k be an **arbitrary integer.**

[TODO!]

Since k(k+3) is even, and k was arbitrary, the claim holds for all integers

Problem 1: Even Steven

Prove that for all integers k, k(k +3) is even.

Predicate logic: $\forall k(Even(k(k + 3)))$

We're a bit stuck here...we don't know anything about k to find a general value of j that will always work. Are there some useful cases we can split into here?

Step 2. Prove it!

Let k be an **arbitrary integer.**

[TODO!]

We found an integer j such that k(k+3)=2j, so by def of even, k(k+3) is even.

Since k(k+3) is even, and k was arbitrary, the claim holds for all integers

note this claim is at the end - we need to get to this point, we can't start with it as that would be backwards!

Problem 1: Even Steven

Now we need to prove the claim in both cases. What information does each case give us?

Prove that for all integers k, k(k +3) is even.

Predicate logic: $\forall k(Even(k(k + 3)))$

Step 2. Prove it!

Let k be an **arbitrary integer.**

Case 1: **k is even**

[TODO!]

We found an integer j such that k(k+3)=2j, so by def of even, k(k+3) is even.

Case 2: **k is odd**

[TODO!]

We found an integer j such that k(k+3)=2j, so by def of even, k(k+3) is even.

Since k(k+3) is even, and k was arbitrary, the claim holds for all integers

Problem 1: Even Steven

Now we need to prove the claim in both cases

Prove that for all integers k, k(k +3) is even.

Predicate logic: $\forall k(Even(k(k + 3)))$

Step 2. Prove it!

Let k be an **arbitrary integer.**
Case 1: **k is even**
By definition there is an integer w such that k = 2w
[TODO!]
We found an integer j such that k(k+3)=2j, so by def of even, k(k+3) is even.

Case 2: **k is odd**
By definition of odd, there is an integer w such that k = 2w+1
[TODO!]
We found an integer j such that k(k+3)=2j, so by def of even, k(k+3) is even.

Since k(k+3) is even, and k was arbitrary, the claim holds for all integers

Problem 1: Even Steven

Plug into the expression we're interested in...

Prove that for all integers k, k(k +3) is even.

Predicate logic: $\forall k(Even(k(k + 3)))$

Step 2. Prove it!

Let k be an **arbitrary integer.**

Case 1: **k is even**

By definition there is an integer w such that k = 2w

Plugging in, $k(k+3)=2w(2w+3)=4w^2 + 6w = 2(w^2+3w)$

[TODO!]

We found an integer j such that k(k+3)=2j, so by def of even, k(k+3) is even.

Case 2: **k is odd**

By definition of odd, there is an integer w such that k = 2w+1

Plugging in, $k(k+3)=(2w+1)(2w+1+3)=(2w+1)(2w+4) = 2(w+2)(2w+4)$

[TODO!]

We found an integer j such that k(k+3)=2j, so by def of even, k(k+3) is even.

Since k(k+3) is even, and k was arbitrary, the claim holds for all integers

Problem 1: Even Steven

Make sure we specify j is an integer

Prove that for all integers k, k(k +3) is even.

Predicate logic: $\forall k(Even(k(k + 3)))$

Step 2. Prove it!

Let k be an **arbitrary integer.**

Case 1: **k is even**

By definition there is an integer w such that $k = 2w$

Plugging in, $k(k+3)=2w(2w+3)=4w^2 + 6w = 2(w^2+3w)$

Let $j = w^2+3w$. j is an integer under the closure of addition and multiplication.

We found an integer j such that $k(k+3)=2j$, so by def of even, k(k+3) is even.

Case 2: **k is odd**

By definition of odd, there is an integer w such that $k = 2w+1$

Plugging in, $k(k+3)=(2w+1)(2w+1+3)=(2w+1)(2w+4) = 2(w+2)(2w+4)$

Let $j = (w+2)(2w+4)$. j is an integer under the closure of addition and multiplication.

We found an integer j such that $k(k+3)=2j$, so by def of even, k(k+3) is even.

Since k(k+3) is even, and k was arbitrary, the claim holds for all integers

Problem 1: Even Steven

done! make sure to read proof again top to bottom to double check:)

Prove that for all integers k, k(k +3) is even.

Predicate logic: $\forall k(Even(k(k + 3)))$

Step 2. Prove it!

Let k be an **arbitrary integer.**

Case 1: **k is even**

By definition there is an integer w such that k = 2w

Plugging in, $k(k+3)=2w(2w+3)=4w^2 + 6w = 2(w^2+3w)$

Let $j = w^2+3w$. j is an integer under the closure of addition and multiplication.

We found an integer j such that k(k+3)=2j, so by def of even, k(k+3) is even.

Case 2: **k is odd**

By definition of odd, there is an integer w such that k = 2w+1

Plugging in, $k(k+3)=(2w+1)(2w+1+3)=(2w+1)(2w+4) = 2(w+2)(2w+4)$

Let j = (w+2)(2w+4). j is an integer under the closure of addition and multiplication.

We found an integer j such that k(k+3)=2j, so by def of even, k(k+3) is even.

Since k(k+3) is even, and k was arbitrary, the claim holds for all integers

Problem 2: Proof by Contradiction

Q2: Proof by Contradiction

Write a proof by contradiction for the following proposition:

There exist no integers x and y such that $18x + 6y = 1$

Step 1. Negate the claim

Step 2. Prove by contradiction

Work on this with the people around you and then we'll go over it together!

Q2: Proof by Contradiction

Write a proof by contradiction for the following proposition:

There exist no integers x and y such that $18x + 6y = 1$

Step 1. Negate the claim

There ***does*** exist an integer x and y such that $18x + 6y = 1$

Step 2. Prove by contradiction

Always start with the template!

Q2: Proof by Contradiction

Write a proof by contradiction for the following proposition:

There exist no integers x and y such that $18x + 6y = 1$

Step 2. Prove by contradiction

Suppose, for the sake of contradiction that there ***does*** exist an integer x and y such that 18x + 6y = 1.

[TODO!]

But this is a contradiction!!

So, **there exists no integers x and y such that $18x + 6y = 1$**

Q2: Proof by Contradiction

Let's play around with the info we get from our suppose..does this expression make sense??

Step 2. Prove by contradiction

Suppose, for the sake of contradiction that there ***does*** exist an integer x and y such that 18x + 6y = 1.

This gives us 18x + 6y = 1. Dividing both sides by 3 gives 6x + 2y = 1/3.

[TODO!]

But this is a contradiction!!

So, **there exists no integers x and y such that $18x + 6y = 1$**

We found the contradiction!

Q2: Proof by Contradiction

Step 2. Prove by contradiction

Suppose, for the sake of contradiction that there ***does*** exist an integer x and y such that 18x + 6y = 1.

This gives us 18x + 6y = 1. Dividing both sides by 3 gives 6x + 2y = 1/3.

x and y are integers meaning that they are closed under add and multiply. But ⅓ is not an integer! This is a contradiction!! 🔥🔥

So, **there exists no integers x and y such that $18x + 6y = 1$**

Problem 3: Number Theory

Problem 3 – 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 $y^2 \equiv 1 \pmod{p}$.

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.

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 $p \mid b$.

Work on this problem with the people around you.

Problem 3 – 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 $y^2 \equiv 1 \pmod{p}$.

Problem 3 – 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 $y^2 \equiv 1 \pmod{p}$.

Claim in predicate logic: $\forall y[(y \equiv 1 \pmod{p}) \rightarrow (y^2 \equiv 1 \pmod{p})]$

Problem 3 – 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 $y^2 \equiv 1 \pmod{p}$.

Claim in predicate logic: $\forall y[(y \equiv 1 \pmod{p}) \rightarrow (y^2 \equiv 1 \pmod{p})]$

Let y be an arbitrary integer and suppose $y \equiv 1 \pmod{p}$.

…

$y^2 \equiv 1 \pmod{p}$.

Since y is arbitrary, the claim holds.

Problem 3 – 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 $y^2 \equiv 1 \pmod{p}$.

Claim in predicate logic: $\forall y[(y \equiv 1 \pmod{p}) \rightarrow (y^2 \equiv 1 \pmod{p})]$

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 $y^2 \equiv 1^2 \pmod{p}$.
$\ldots y^2 \equiv 1 \pmod{p}$
Since y is arbitrary, the claim holds.

Problem 3 – 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 $y^2 \equiv 1 \pmod{p}$.

Claim in predicate logic: $\forall y[(y \equiv 1 \pmod{p}) \rightarrow (y^2 \equiv 1 \pmod{p})]$

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 $y^2 \equiv 1^2 \pmod{p}$.
Simplifying, we have $y^2 \equiv 1 \pmod{p}$
Since y is arbitrary, the claim holds.

Problem 3 – Number Theory

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

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.

Problem 3 – Number Theory

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

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.

Let x be an arbitrary integer and suppose $x \equiv 1 \pmod{p}$.

…

$x^2 \equiv 1 \pmod{p}$.

Since x was arbitrary, the claim holds.

Problem 3 – Number Theory

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

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.

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 $pk = (x - 1)$.

…

$x^2 \equiv 1 \pmod{p}$.
Since x was arbitrary, the claim holds.

Problem 3 – Number Theory

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

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.

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 $(x+1)$, we have $pk(x+1) = (x-1)(x+1)$.
…

$x^2 \equiv 1 \pmod{p}$.
Since x was arbitrary, the claim holds.

Problem 3 – Number Theory

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

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.

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 $(x+1)$, we have $pk(x+1) = (x-1)(x+1)$.
Rearranging the equation, we have $p(k(x+1)) = (x-1)(x+1)$.
…

$x^2 \equiv 1 \pmod{p}$.
Since x was arbitrary, the claim holds.

Problem 3 – Number Theory

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

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.

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 $(x+1)$, we have $pk(x+1) = (x-1)(x+1)$.
Rearranging the equation, we have $p(k(x+1)) = (x-1)(x+1)$.

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

…
$x^2 \equiv 1 \pmod{p}$.
Since x was arbitrary, the claim holds.

Problem 3 – Number Theory

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

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.

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 $(x+1)$, we have $pk(x+1) = (x-1)(x+1)$.
Rearranging the equation, we have $p(k(x+1)) = (x-1)(x+1)$.

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, $p \mid x^2 - 1$.
$\ldots x^2 \equiv 1 \pmod{p}$.
Since x was arbitrary, the claim holds.

Problem 3 – Number Theory

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

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.

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 $(x+1)$, we have $pk(x+1) = (x-1)(x+1)$.
Rearranging the equation, we have $p(k(x+1)) = (x-1)(x+1)$.

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, $x^2 \equiv 1 \pmod{p}$.
Since x was arbitrary, the claim holds.

Problem 3 – Number Theory

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

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 $p \mid b$.

Problem 3 – Number Theory

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

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 $p \mid b$.

Let x be an arbitrary integer and suppose $x^2 \equiv 1 \pmod{p}$.

…

$x \equiv 1 \pmod{p}$ or $x \equiv -1 \pmod{p}$.
Since x was arbitrary, the claim holds.

Problem 3 – Number Theory

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

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 $p \mid b$.

Let x be an arbitrary integer and suppose $x^2 \equiv 1 \pmod{p}$.

By the definition of Congruences, $p \mid x^2 - 1$.
…

$x \equiv 1 \pmod{p}$ or $x \equiv -1 \pmod{p}$.
Since x was arbitrary, the claim holds.

Problem 3 – Number Theory

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

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 $p \mid b$.

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 $p \mid (x-1)(x+1)$
…

$x \equiv 1 \pmod{p}$ or $x \equiv -1 \pmod{p}$.
Since x was arbitrary, the claim holds.

Problem 3 – Number Theory

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

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 $p \mid b$.

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 $p \mid b$.
…

$x \equiv 1 \pmod{p}$ or $x \equiv -1 \pmod{p}$.
Since x was arbitrary, the claim holds.

Problem 3 – Number Theory

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

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 $p \mid b$.

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 $p \mid (x+1)$.

$\ldots x \equiv 1 \pmod{p}$ or $x \equiv -1 \pmod{p}$.
Since x was arbitrary, the claim holds.

Problem 3 – Number Theory

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

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 $p \mid b$.

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 $x \equiv -1 \pmod{p}$.
Since x was arbitrary, the claim holds.

Problem 4: Induction

Problem 4 – 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 $n \in \mathbb{N}$, $S_n = \frac{1}{6}n(n+1)(2n+1)$.

Work on this problem with the people around you.

Problem 4 – Induction

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

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

Let $P(n)$ be "". We show $P(n)$ holds for (some) n by induction on n.

Base Case: $P(b)$:

Inductive Hypothesis: Suppose $P(k)$ holds for an arbitrary $k \geq b$.

Inductive Step: Goal: Show $P(k+1)$:

Conclusion: Therefore, $P(n)$ holds for (some) n by the principle of induction.

Problem 4 – Induction

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

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

Let $P(n)$ be "$S_n = \frac{1}{6}n(n+1)(2n+1)$". We show $P(n)$ holds for all $n \in \mathbb{N}$ by induction on n.

Base Case: $P(b)$:

Inductive Hypothesis: Suppose $P(k)$ holds for an arbitrary $k \geq b$

Inductive Step: Goal: Show $P(k+1)$:

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

Problem 4 – Induction

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

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

Let $P(n)$ be "$S_n = \frac{1}{6}n(n+1)(2n+1)$". We show $P(n)$ holds for all $n \in \mathbb{N}$ by induction on n.

Base Case: $P(0)$: When $n = 0$, 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 $\frac{1}{6}(0)(0+1)(2 \cdot 0 + 1)$, we know that $P(0)$ is true.

Inductive Hypothesis: Suppose $P(k)$ holds for an arbitrary $k \geq b$

Inductive Step: Goal: Show $P(k+1)$:

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

Problem 4 – Induction

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

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

Let $P(n)$ be "$S_n = \frac{1}{6}n(n+1)(2n+1)$". We show $P(n)$ holds for all $n \in \mathbb{N}$ by induction on n.

Base Case: $P(0)$: When $n = 0$, 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 $\frac{1}{6}(0)(0+1)(2 \cdot 0 + 1)$, we know that $P(0)$ is true.

Inductive Hypothesis: Suppose $P(k)$ holds for an arbitrary $k \geq 0$, i.e. $S_k = \frac{1}{6}k(k+1)(2k+1)$

Inductive Step: Goal: Show $P(k+1)$:

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

Problem 4 – Induction

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

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

Let $P(n)$ be "$S_n = \frac{1}{6}n(n+1)(2n+1)$". We show $P(n)$ holds for all $n \in \mathbb{N}$ by induction on n.

Base Case: $P(0)$: When $n = 0$, 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 $\frac{1}{6}(0)(0+1)(2 \cdot 0 + 1)$, we know that $P(0)$ is true.

Inductive Hypothesis: Suppose $P(k)$ holds for an arbitrary $k \geq 0$, i.e. $S_k = \frac{1}{6}k(k+1)(2k+1)$

Inductive Step: Goal: Show $P(k+1)$: $S_{k+1} = \frac{1}{6}(k+1)((k+1)+1)(2(k+1)+1)$

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

Problem 4 – Induction

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

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

Let $P(n)$ be "$S_n = \frac{1}{6}n(n+1)(2n+1)$". We show $P(n)$ holds for all $n \in \mathbb{N}$ by induction on n.

Base Case: $P(0)$: When $n = 0$, 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 $\frac{1}{6}(0)(0+1)(2 \cdot 0 + 1)$, we know that $P(0)$ is true.

Inductive Hypothesis: Suppose $P(k)$ holds for an arbitrary $k \geq 0$, i.e. $S_k = \frac{1}{6}k(k+1)(2k+1)$

Inductive Step: Goal: Show $P(k+1)$: $S_{k+1} = \frac{1}{6}(k+1)((k+1)+1)(2(k+1)+1)$

$$\begin{aligned} S_{k+1} &= \\ &= \cdots \\ &= \frac{1}{6}(k+1)((k+1)+1)(2(k+1)+1) \end{aligned}$$

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

Problem 4 – Induction

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

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

Let $P(n)$ be "$S_n = \frac{1}{6}n(n+1)(2n+1)$". We show $P(n)$ holds for all $n \in \mathbb{N}$ by induction on n.

Base Case: $P(0)$: When $n = 0$, 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 $\frac{1}{6}(0)(0+1)(2 \cdot 0 + 1)$, we know that $P(0)$ is true.

Inductive Hypothesis: Suppose $P(k)$ holds for an arbitrary $k \geq 0$, i.e. $S_k = \frac{1}{6}k(k+1)(2k+1)$

Inductive Step: Goal: Show $P(k+1)$: $S_{k+1} = \frac{1}{6}(k+1)((k+1)+1)(2(k+1)+1)$

$$S_{k+1} = 1^2 + 2^2 + \cdots + k^2 + (k+1)^2 \qquad \text{by definition of } S_n$$
$$= \cdots$$
$$= \frac{1}{6}(k+1)((k+1)+1)(2(k+1)+1)$$

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

Problem 4 – Induction

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

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

Let $P(n)$ be "$S_n = \frac{1}{6}n(n+1)(2n+1)$". We show $P(n)$ holds for all $n \in \mathbb{N}$ by induction on n.

Base Case: $P(0)$: When $n = 0$, 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 $\frac{1}{6}(0)(0+1)(2 \cdot 0 + 1)$, we know that $P(0)$ is true.

Inductive Hypothesis: Suppose $P(k)$ holds for an arbitrary $k \geq 0$, i.e. $S_k = \frac{1}{6}k(k+1)(2k+1)$

Inductive Step: Goal: Show $P(k+1)$: $S_{k+1} = \frac{1}{6}(k+1)((k+1)+1)(2(k+1)+1)$

$$\begin{aligned} S_{k+1} &= 1^2 + 2^2 + \cdots + k^2 + (k+1)^2 && \text{by definition of } S_n \\ &= (1^2 + 2^2 + \cdots + k^2) + (k+1)^2 \\ &= \cdots \\ &= \tfrac{1}{6}(k+1)((k+1)+1)(2(k+1)+1) \end{aligned}$$

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

Problem 4 – Induction

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

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

Let $P(n)$ be "$S_n = \frac{1}{6}n(n+1)(2n+1)$". We show $P(n)$ holds for all $n \in \mathbb{N}$ by induction on n.

Base Case: $P(0)$: When $n = 0$, 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 $\frac{1}{6}(0)(0+1)(2 \cdot 0 + 1)$, we know that $P(0)$ is true.

Inductive Hypothesis: Suppose $P(k)$ holds for an arbitrary $k \geq 0$, i.e. $S_k = \frac{1}{6}k(k+1)(2k+1)$

Inductive Step: Goal: Show $P(k+1)$: $S_{k+1} = \frac{1}{6}(k+1)((k+1)+1)(2(k+1)+1)$

$$
\begin{aligned}
S_{k+1} &= 1^2 + 2^2 + \cdots + k^2 + (k+1)^2 && \text{by definition of } S_n \\
&= (1^2 + 2^2 + \cdots + k^2) + (k+1)^2 \\
&= S_k + (k+1)^2 && \text{by definition of } S_n \\
&= \cdots \\
&= \tfrac{1}{6}(k+1)((k+1)+1)(2(k+1)+1)
\end{aligned}
$$

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

Problem 4 – Induction

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

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

Let $P(n)$ be "$S_n = \frac{1}{6}n(n+1)(2n+1)$". We show $P(n)$ holds for all $n \in \mathbb{N}$ by induction on n.

Base Case: $P(0)$: When $n = 0$, 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 $\frac{1}{6}(0)(0+1)(2 \cdot 0 + 1)$, we know that $P(0)$ is true.

Inductive Hypothesis: Suppose $P(k)$ holds for an arbitrary $k \geq 0$, i.e. $S_k = \frac{1}{6}k(k+1)(2k+1)$

Inductive Step: Goal: Show $P(k+1)$: $S_{k+1} = \frac{1}{6}(k+1)((k+1)+1)(2(k+1)+1)$

$$
\begin{aligned}
S_{k+1} &= 1^2 + 2^2 + \cdots + k^2 + (k+1)^2 && \text{by definition of } S_n \\
&= (1^2 + 2^2 + \cdots + k^2) + (k+1)^2 \\
&= S_k + (k+1)^2 && \text{by definition of } S_n \\
&= \tfrac{1}{6}k(k+1)(2k+1) + (k+1)^2 && \text{by I.H.} \\
&= \cdots \\
&= \tfrac{1}{6}(k+1)((k+1)+1)(2(k+1)+1)
\end{aligned}
$$

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

Problem 4 – Induction

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

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

Let $P(n)$ be "$S_n = \frac{1}{6}n(n+1)(2n+1)$". We show $P(n)$ holds for all $n \in \mathbb{N}$ by induction on n.

Base Case: $P(0)$: When $n = 0$, 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 $\frac{1}{6}(0)(0+1)(2 \cdot 0 + 1)$, we know that $P(0)$ is true.

Inductive Hypothesis: Suppose $P(k)$ holds for an arbitrary $k \geq 0$, i.e. $S_k = \frac{1}{6}k(k+1)(2k+1)$

Inductive Step: Goal: Show $P(k+1)$: $S_{k+1} = \frac{1}{6}(k+1)((k+1)+1)(2(k+1)+1)$

$$
\begin{aligned}
S_{k+1} &= 1^2 + 2^2 + \cdots + k^2 + (k+1)^2 && \text{by definition of } S_n \\
&= (1^2 + 2^2 + \cdots + k^2) + (k+1)^2 \\
&= S_k + (k+1)^2 && \text{by definition of } S_n \\
&= \tfrac{1}{6}k(k+1)(2k+1) + (k+1)^2 && \text{by I.H.} \\
&= (k+1)(\tfrac{1}{6}k(2k+1) + (k+1)) \\
&= \cdots \\
&= \tfrac{1}{6}(k+1)((k+1)+1)(2(k+1)+1)
\end{aligned}
$$

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

Problem 4 – Induction

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

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

Let $P(n)$ be "$S_n = \frac{1}{6}n(n+1)(2n+1)$". We show $P(n)$ holds for all $n \in \mathbb{N}$ by induction on n.

Base Case: $P(0)$: When $n = 0$, 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 $\frac{1}{6}(0)(0+1)(2 \cdot 0 + 1)$, we know that $P(0)$ is true.

Inductive Hypothesis: Suppose $P(k)$ holds for an arbitrary $k \geq 0$, i.e. $S_k = \frac{1}{6}k(k+1)(2k+1)$

Inductive Step: Goal: Show $P(k+1)$: $S_{k+1} = \frac{1}{6}(k+1)((k+1)+1)(2(k+1)+1)$

$$
\begin{aligned}
S_{k+1} &= 1^2 + 2^2 + \cdots + k^2 + (k+1)^2 && \text{by definition of } S_n \\
&= (1^2 + 2^2 + \cdots + k^2) + (k+1)^2 \\
&= S_k + (k+1)^2 && \text{by definition of } S_n \\
&= \tfrac{1}{6}k(k+1)(2k+1) + (k+1)^2 && \text{by I.H.} \\
&= (k+1)(\tfrac{1}{6}k(2k+1) + (k+1)) \\
&= \tfrac{1}{6}(k+1)(k(2k+1) + 6(k+1)) \\
&= \cdots \\
&= \tfrac{1}{6}(k+1)((k+1)+1)(2(k+1)+1)
\end{aligned}
$$

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

Problem 4 – Induction

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

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

Let $P(n)$ be "$S_n = \frac{1}{6}n(n+1)(2n+1)$". We show $P(n)$ holds for all $n \in \mathbb{N}$ by induction on n.

Base Case: $P(0)$: When $n = 0$, 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 $\frac{1}{6}(0)(0+1)(2 \cdot 0 + 1)$, we know that $P(0)$ is true.

Inductive Hypothesis: Suppose $P(k)$ holds for an arbitrary $k \geq 0$, i.e. $S_k = \frac{1}{6}k(k+1)(2k+1)$

Inductive Step: Goal: Show $P(k+1)$: $S_{k+1} = \frac{1}{6}(k+1)((k+1)+1)(2(k+1)+1)$

$$
\begin{aligned}
S_{k+1} &= 1^2 + 2^2 + \cdots + k^2 + (k+1)^2 && \text{by definition of } S_n \\
&= (1^2 + 2^2 + \cdots + k^2) + (k+1)^2 \\
&= S_k + (k+1)^2 && \text{by definition of } S_n \\
&= \tfrac{1}{6}k(k+1)(2k+1) + (k+1)^2 && \text{by I.H.} \\
&= (k+1)(\tfrac{1}{6}k(2k+1) + (k+1)) \\
&= \tfrac{1}{6}(k+1)(k(2k+1) + 6(k+1)) \\
&= \tfrac{1}{6}(k+1)(2k^2 + k + 6k + 6) \\
&= \cdots \\
&= \tfrac{1}{6}(k+1)((k+1)+1)(2(k+1)+1)
\end{aligned}
$$

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

Problem 4 – Induction

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

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

Let $P(n)$ be "$S_n = \frac{1}{6}n(n+1)(2n+1)$". We show $P(n)$ holds for all $n \in \mathbb{N}$ by induction on n.

Base Case: $P(0)$: When $n = 0$, 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 $\frac{1}{6}(0)(0+1)(2 \cdot 0 + 1)$, we know that $P(0)$ is true.

Inductive Hypothesis: Suppose $P(k)$ holds for an arbitrary $k \geq 0$, i.e. $S_k = \frac{1}{6}k(k+1)(2k+1)$

Inductive Step: Goal: Show $P(k+1)$: $S_{k+1} = \frac{1}{6}(k+1)((k+1)+1)(2(k+1)+1)$

$$
\begin{aligned}
S_{k+1} &= 1^2 + 2^2 + \cdots + k^2 + (k+1)^2 && \text{by definition of } S_n \\
&= (1^2 + 2^2 + \cdots + k^2) + (k+1)^2 \\
&= S_k + (k+1)^2 && \text{by definition of } S_n \\
&= \tfrac{1}{6}k(k+1)(2k+1) + (k+1)^2 && \text{by I.H.} \\
&= (k+1)(\tfrac{1}{6}k(2k+1) + (k+1)) \\
&= \tfrac{1}{6}(k+1)(k(2k+1) + 6(k+1)) \\
&= \tfrac{1}{6}(k+1)(2k^2 + k + 6k + 6) \\
&= \tfrac{1}{6}(k+1)(2k^2 + 7k + 6) \\
&= \cdots \\
&= \tfrac{1}{6}(k+1)((k+1)+1)(2(k+1)+1)
\end{aligned}
$$

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

Problem 4 – Induction

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

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

Let $P(n)$ be "$S_n = \frac{1}{6}n(n+1)(2n+1)$". We show $P(n)$ holds for all $n \in \mathbb{N}$ by induction on n.

Base Case: $P(0)$: When $n = 0$, 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 $\frac{1}{6}(0)(0+1)(2 \cdot 0 + 1)$, we know that $P(0)$ is true.

Inductive Hypothesis: Suppose $P(k)$ holds for an arbitrary $k \geq 0$, i.e. $S_k = \frac{1}{6}k(k+1)(2k+1)$

Inductive Step: Goal: Show $P(k+1)$: $S_{k+1} = \frac{1}{6}(k+1)((k+1)+1)(2(k+1)+1)$

$$
\begin{aligned}
S_{k+1} &= 1^2 + 2^2 + \cdots + k^2 + (k+1)^2 && \text{by definition of } S_n \\
&= (1^2 + 2^2 + \cdots + k^2) + (k+1)^2 \\
&= S_k + (k+1)^2 && \text{by definition of } S_n \\
&= \tfrac{1}{6}k(k+1)(2k+1) + (k+1)^2 && \text{by I.H.} \\
&= (k+1)(\tfrac{1}{6}k(2k+1) + (k+1)) \\
&= \tfrac{1}{6}(k+1)(k(2k+1) + 6(k+1)) \\
&= \tfrac{1}{6}(k+1)(2k^2 + k + 6k + 6) \\
&= \tfrac{1}{6}(k+1)(2k^2 + 7k + 6) \\
&= \tfrac{1}{6}(k+1)(k+2)(2k+3) \\
&= \tfrac{1}{6}(k+1)((k+1)+1)(2(k+1)+1)
\end{aligned}
$$

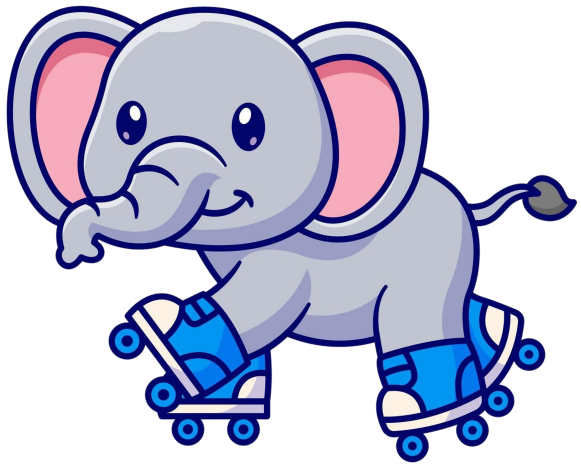
Conclusion: Therefore, $P(n)$ holds for all $n \in \mathbb{N}$ by the principle of induction.

Problem 5: Strong Induction

Problem 5 – 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 $n \geq 24$



Work on this problem with the people around you.

Problem 5 – Strong Induction

Can buy snacks in packs of 5 and packs of 7.
Prove that Robbie can buy exactly n snacks for all integers $n \geq 24$

Let $P(n)$ be "".

We show $P(n)$ holds for all $n \geq b_{min}$ by strong induction on n.

Base Cases:

Inductive Hypothesis: Suppose $P(b_{min}) \wedge \cdots \wedge P(k)$ hold for an arbitrary all $k \geq b_{max}$.

Inductive Step: Goal: Show $P(k+1)$:

Conclusion: Therefore, $P(n)$ holds for all $n \geq b_{min}$ by the principle of induction.

Problem 5 – Strong Induction

Can buy snacks in packs of 5 and packs o
7.
Prove that Robbie can buy exactly n
snacks for all integers $n \geq 24$

Let $P(n)$ be "Robbie can buy exactly n snacks with packs of 5 and 7".

We show $P(n)$ holds for all $n \geq 24$ by strong induction on n.

Base Cases:

Inductive Hypothesis: Suppose $P(b_{min}) \wedge \cdots \wedge P(k)$ hold for an arbitrary all $k \geq b_{max}$.

Inductive Step: Goal: Show $P(k+1)$:

Conclusion: Therefore, $P(n)$ holds for all $n \geq 24$ by the principle of induction.

Problem 5 – Strong Induction

Can buy snacks in packs of 5 and packs o
7.
Prove that Robbie can buy exactly n
snacks for all integers $n \geq 24$

Let $P(n)$ be "Robbie can buy exactly n snacks with packs of 5 and 7".

We show $P(n)$ holds for all $n \geq 24$ by strong induction on n.

Base Cases:

Inductive Hypothesis: Suppose $P(b_{min}) \wedge \cdots \wedge P(k)$ hold for an arbitrary all $k \geq b_{max}$.

Inductive Step: Goal: Show $P(k+1)$:

Conclusion: Therefore, $P(n)$ holds for all $n \geq 24$ by the principle of induction.

How can we tell how many base cases we need?

The smallest number of snacks we can add at one time is 5. This tells us we probably need 5 base cases, because then the 6th case can be reached by adding 5 to the minimum base case

Problem 5 – Strong Induction

Can buy snacks in packs of 5 and packs o
7.
Prove that Robbie can buy exactly n
snacks for all integers $n \geq 24$

Let $P(n)$ be "Robbie can buy exactly n snacks with packs of 5 and 7".

We show $P(n)$ holds for all $n \geq 24$ by strong induction on n.

Base Cases: $n = 24$: 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 $P(b_{min}) \wedge \cdots \wedge P(k)$ hold for an arbitrary all $k \geq b_{max}$.

Inductive Step: Goal: Show $P(k+1)$:

Conclusion: Therefore, $P(n)$ holds for all $n \geq 24$ by the principle of induction.

Problem 5 – Strong Induction

Can buy snacks in packs of 5 and packs o
7.
Prove that Robbie can buy exactly n
snacks for all integers $n \geq 24$

Let $P(n)$ be "Robbie can buy exactly n snacks with packs of 5 and 7".

We show $P(n)$ holds for all $n \geq 24$ by strong induction on n.

Base Cases: $n = 24$: 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 $P(24) \wedge P(25) \wedge \cdots \wedge P(k)$ hold for an arbitrary all $k \geq 28$.

Inductive Step: Goal: Show $P(k+1)$:

Conclusion: Therefore, $P(n)$ holds for all $n \geq 24$ by the principle of induction.

Problem 5 – Strong Induction

Can buy snacks in packs of 5 and packs o
7.
Prove that Robbie can buy exactly n
snacks for all integers $n \geq 24$

Let $P(n)$ be "Robbie can buy exactly n snacks with packs of 5 and 7".

We show $P(n)$ holds for all $n \geq 24$ by strong induction on n.

Base Cases: $n = 24$: 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 $P(24) \wedge P(25) \wedge \cdots \wedge P(k)$ hold for an arbitrary all $k \geq 28$.

Inductive Step: Goal: Show $P(k+1)$: Robbie can buy exactly $k+1$ snacks with packs of 5 and 7.

…

Conclusion: Therefore, $P(n)$ holds for all $n \geq 24$ by the principle of induction.

Problem 5 – Strong Induction

Can buy snacks in packs of 5 and packs o
7.
Prove that Robbie can buy exactly n
snacks for all integers $n \geq 24$

Let $P(n)$ be "Robbie can buy exactly n snacks with packs of 5 and 7".

We show $P(n)$ holds for all $n \geq 24$ by strong induction on n.

Base Cases: $n = 24$: 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 $P(24) \wedge P(25) \wedge \cdots \wedge P(k)$ hold for an arbitrary all $k \geq 28$.

Inductive Step: Goal: Show $P(k+1)$: Robbie can buy exactly $k+1$ snacks with packs of 5 and 7.

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, $P(n)$ holds for all $n \geq 24$ by the principle of induction.

Problem 6: Reversing a Binary Tree

Q6 - Reversing a Binary Tree

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 int, then Tree(x, L, R) is a Tree.

The **sum function** returns the sum of all elements in a Tree.

- sum(Nil) = 0
- sum(Tree(x, L, R)) = x + sum(L) + sum(R)

The **reverse function** produces the mirror image of a Tree.

- reverse(Nil) = Nil
- reverse(Tree(x, L, R)) = Tree(x,reverse(R),reverse(L))

Show that, for all Trees T that sum(T) = sum(reverse(T))

What's a good proof method here...

Q6 - 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 int, then Tree(x, L, R) is a Tree.

The **sum function** returns the sum of all elements in a Tree.

- sum(Nil) = 0
- sum(Tree(x, L, R)) = x + sum(L) + sum(R)

The **reverse function** produces the mirror image of a Tree.

- reverse(Nil) = Nil
- reverse(Tree(x, L, R)) = Tree(x,reverse(R),reverse(L))

Show that, for all Trees T that sum(T) = sum(reverse(T))

Work on this with the people around you and then we'll go over it together!

Let's make the template

Q6 - Reversing a Binary Tree

Show that, for all Trees T that sum(T) = sum(reverse(T))

Let $P(x)$ be "<predicate>". We show $P(x)$ holds for all $x \in S$ by structural induction.

Base Case: Show $P(x)$
[Do that for every base cases x in S.]

Inductive Hypothesis: Suppose $P(x)$ for an arbitrary x
[Do that for every x listed as in S in the recursive rules.]

Inductive Step: Show $P()$ holds for y.
[You will need a separate case/step for every recursive rule.]

Therefore $P(x)$ holds for all $x \in S$ by the principle of induction.

Let's make the template

Q6 - Reversing a Binary Tree

Show that, for all Trees T that sum(T) = sum(reverse(T))

Let ***P*(T) be "sum(T)=sum(reverse(T))"**. We **show *P*(x) for all trees T** by structural induction.

Base Case: Show $P(x)$
[Do that for every base cases x in S.]

Inductive Hypothesis: Suppose $P(x)$ for an arbitrary x
[Do that for every x listed as in S in the recursive rules.]

Inductive Step: Show $P()$ holds for y.
[You will need a separate case/step for every recursive rule.]

Therefore $P(x)$ holds for all $x \in S$ by the principle of induction.

Q6 - Reversing a Binary Tree

Reference the set definition! Remember we are proving the claim about each element as we add to the set

Show that, for all Trees T that sum(T) = sum(reverse(T))

Let ***P*(T) be "sum(T)=sum(reverse(T))"**. We **show *P*(x) for all trees T** by structural induction.

Base Case: Show $P(x)$
[Do that for every base cases x in S.]

Inductive Hypothesis: Suppose $P(x)$ for an arbitrary x
[Do that for every x listed as in S in the recursive rules.]

Inductive Step: Show $P()$ holds for y.
[You will need a separate case/step for every recursive rule.]

Therefore $P(x)$ holds for all $x \in S$ by the principle of induction.

Basis Step: Nil is a Tree.
Recursive Step If L is a Tree, R is a Tree, and x is an int, then Tree(x, L, R) is a Tree.

Q6 - Reversing a Binary Tree

in base case, we prove the claim for the first element added in basis step

Show that, for all Trees T that sum(T) = sum(reverse(T))

Let ***P*(T) be "sum(T)=sum(reverse(T))"**. We **show *P*(x) for all trees T** by structural induction.

Base Case: Show ***P*(Nil)**

Inductive Hypothesis: Suppose $P(x)$ for an arbitrary x
[Do that for every x listed as in S in the recursive rules.]

Inductive Step: Show $P()$ holds for y.
[You will need a separate case/step for every recursive rule.]

Therefore $P(x)$ holds for all $x \in S$ by the principle of induction.

Basis Step: Nil is a Tree.
Recursive Step If L is a Tree, R is a Tree, and x is an int, then Tree(x, L, R) is a Tree.

Q6 - Reversing a Binary Tree

IH should match up with the set elements needed to construct the new element(s) based on recursive step

Show that, for all Trees T that sum(T) = sum(reverse(T))

Let P(T) be "sum(T)=sum(reverse(T))". We show $P(x)$ for all trees T by structural induction.

Base Case: Show P(Nil)

Inductive Hypothesis: Suppose **P(L)** and **P(R)** for an **arbitrary trees L and R**

Inductive Step: Show **P(Tree(x, L, R))** holds for **an arbitrary integer x**

Therefore $P(x)$ holds for all $x \in S$ by the principle of induction.

Basis Step: Nil is a Tree.
Recursive Step If **L is a Tree, R is a Tree**, and **x is an int**, then **Tree(x, L, R)** is a Tree.

Q6 - Reversing a Binary Tree

IS should match up with new element(s) created with recursive step

Show that, for all Trees T that sum(T) = sum(reverse(T))

Let P(T) be "sum(T)=sum(reverse(T))". We show $P(x)$ for all trees T by structural induction.

Base Case: Show P(Nil)

Inductive Hypothesis: Suppose ***P*(L)** and ***P*(R)** for an **arbitrary trees L and R**

Inductive Step: Show ***P*(Tree(x, L, R))** holds for **an arbitrary integer x**

Therefore $P(x)$ holds for all $x \in S$ by the principle of induction.

Basis Step: Nil is a Tree.
Recursive Step If ***L* is a Tree, *R* is a Tree**, and ***x* is an int**, then **Tree(x, L, R)** is a Tree.

Let's fill it in!

Q6 - Reversing a Binary Tree

Show that, for all Trees T that sum(T) = sum(reverse(T))

Let P(T) be "sum(T)=sum(reverse(T))". We show P(T) for all trees T by structural induction.

Base Case: ***Show P(Nil)***

Inductive Hypothesis: ***Suppose P(L) and P(R) for an arbitrary trees L and R***

Inductive Step: ***Show P(Tree(x, L, R)) holds for an arbitrary integer x***

Therefore ***P(T) for all trees T by structural induction***.

Q6 - Reversing a Binary Tree

Base case…use the base case definitions of functions

Show that, for all Trees T that sum(T) = sum(reverse(T))

Let P(T) be "sum(T)=sum(reverse(T))". We show P(T) for all trees T by structural induction.

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

Inductive Hypothesis: ***Suppose $P(L)$ and $P(R)$ for an arbitrary trees L and R***

Inductive Step: ***Show $P(Tree(x, L, R))$ holds for an arbitrary integer x***

Therefore P(T) for all trees T by structural induction.

Q6 - Reversing a Binary Tree

Show that, for all Trees T that sum(T) = sum(reverse(T))

Let P(T) be "sum(T)=sum(reverse(T))". We show P(T) for all trees T by structural induction.

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

Inductive Hypothesis: **Suppose P(L) and P(R) for an arbitrary trees L and R**

Inductive Step: ***Show P(Tree(x, L, R)) holds for an arbitrary integer x***

Therefore P(T) for all trees T by structural induction.

Write the start and end

Q6 - Reversing a Binary Tree

Show that, for all Trees T that sum(T) = sum(reverse(T))

Let P(T) be "sum(T)=sum(reverse(T))". We show P(T) for all trees T by structural induction.

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

Inductive Hypothesis: Suppose P(L) and P(R) for an arbitrary trees L and R

Inductive Step: **Goal: Show P(Tree(x, L, R)) holds for an arbitrary integer x**
sum(reverse(Tree(x, L, R))) = ...
= sum(Tree(x, L, R)) [Definition of sum]

Therefore P(T) for all trees T by structural induction.

apply definitions...

Q6 - Reversing a Binary Tree

Show that, for all Trees T that sum(T) = sum(reverse(T))

Let P(T) be "sum(T)=sum(reverse(T))". We show P(T) for all trees T by structural induction.

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

Inductive Hypothesis: Suppose P(L) and P(R) for an arbitrary trees L and R

Inductive Step: Goal: Show P(Tree(x, L, R)) holds for an arbitrary integer x

sum(reverse(Tree(x, L, R))) = **sum(Tree(x,reverse(R),reverse(L))) [Definition of reverse]**

.....

= sum(Tree(x, L, R)) [Definition of sum]

Therefore P(T) for all trees T by structural induction.

apply definitions...

Q6 - Reversing a Binary Tree

Show that, for all Trees T that sum(T) = sum(reverse(T))

Let P(T) be "sum(T)=sum(reverse(T))". We show P(T) for all trees T by structural induction.

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

Inductive Hypothesis: Suppose P(L) and P(R) for an arbitrary trees L and R

Inductive Step: Goal: Show P(Tree(x, L, R)) holds for an arbitrary integer x

sum(reverse(Tree(x, L, R))) = sum(Tree(x,reverse(R),reverse(L))) [Definition of reverse]

= x + sum(reverse(R)) + sum(reverse(L)) [Definition of sum]

.....

= sum(Tree(x, L, R)) [Definition of sum]

Therefore P(T) for all trees T by structural induction.

this matches form of IH!

Q6 - Reversing a Binary Tree

Show that, for all Trees T that sum(T) = sum(reverse(T))

Let P(T) be "sum(T)=sum(reverse(T))". We show P(T) for all trees T by structural induction.

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

Inductive Hypothesis: Suppose P(L) and P(R) for an arbitrary trees L and R

Inductive Step: Goal: Show P(Tree(x, L, R)) holds for an arbitrary integer x

sum(reverse(Tree(x, L, R))) = sum(Tree(x,reverse(R),reverse(L))) [Definition of reverse]

= x + sum(reverse(R)) + sum(reverse(L)) [Definition of sum]

= x + sum(R) + sum(L) [Inductive Hypothesis]

....

= sum(Tree(x, L, R)) [Definition of sum]

Therefore P(T) for all trees T by structural induction.

Q6 - Reversing a Binary Tree

Get into exactly same format as P(...)

Show that, for all Trees T that sum(T) = sum(reverse(T))

Let P(T) be "sum(T)=sum(reverse(T))". We show P(T) for all trees T by structural induction.

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

Inductive Hypothesis: Suppose P(L) and P(R) for an arbitrary trees L and R

Inductive Step: Goal: Show P(Tree(x, L, R)) holds for an arbitrary integer x

sum(reverse(Tree(x, L, R))) = sum(Tree(x,reverse(R),reverse(L))) [Definition of reverse]

= x + sum(reverse(R)) + sum(reverse(L)) [Definition of sum]

= x + sum(R) + sum(L) [Inductive Hypothesis]

= x + sum(L) + sum(R) [Commutativity]

= sum(Tree(x, L, R)) [Definition of sum]

Therefore P(T) for all trees T by structural induction.

admire the proof 🤩

Q6 - Reversing a Binary Tree

Show that, for all Trees T that sum(T) = sum(reverse(T))

Let P(T) be "sum(T)=sum(reverse(T))". We show P(T) for all trees T by structural induction.

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

Inductive Hypothesis: Suppose P(L) and P(R) for an arbitrary trees L and R

Inductive Step: Goal: Show P(Tree(x, L, R)) holds for an arbitrary integer x

sum(reverse(Tree(x, L, R))) = sum(Tree(x,reverse(R),reverse(L))) [Definition of reverse]

= x + sum(reverse(R)) + sum(reverse(L)) [Definition of sum]

= x + sum(R) + sum(L) [Inductive Hypothesis]

= x + sum(L) + sum(R) [Commutativity]

= sum(Tree(x, L, R)) [Definition of sum]

This shows P(Tree(x, L, R)).

Therefore P(T) for all trees T by structural induction.

Problem 7: Unioned Intersections

Q7 - Unioned Intersections

Show that there exists sets A, B, C, D, E, F such that $(A \cap B) \cup (C \cap D) \cup (E \cap F) \nsubseteq (A \cup B) \cap (C \cup D) \cap (E \cup F)$.

What's a good proof method here...

Q7 - Unioned Intersections

Show that there exists sets A, B, C, D, E, F such that $(A \cap B) \cup (C \cap D) \cup (E \cap F) \not\subseteq (A \cup B) \cap (C \cup D) \cap (E \cup F)$.

Proof by example!
we just need to give an example to show “there exists”

Q7 - Unioned Intersections

Show that there exists sets A, B, C, D, E, F such that $(A \cap B) \cup (C \cap D) \cup (E \cap F) \not\subseteq (A \cup B) \cap (C \cup D) \cap (E \cup F)$.

Proof by example!
we just need to give an example to show "there exists"

Work on this with the people around you and then we'll go over it together!

Q7 - Unioned Intersections

before doing a proof by example, think about intuitively why the claim is true or false. this helps guide us when finding an example!

Show that there exists sets A, B, C, D, E, F such that
$(A \cap B) \cup (C \cap D) \cup (E \cap F) \not\subseteq (A \cup B) \cap (C \cup D) \cap (E \cup F)$.

Intuitively, why does this prove not work?

Q7 - Unioned Intersections

before doing a proof by example, think about intuitively why the claim is true or false. this helps guide us when finding an example!

Show that there exists sets A, B, C, D, E, F such that
$(A \cap B) \cup (C \cap D) \cup (E \cap F) \not\subseteq (A \cup B) \cap (C \cup D) \cap (E \cup F)$.

Intuitively, why does this prove not work?

For an element to be part of the set on the left, in need to be in at least one of the unioned sets - maybe it's in $A \cap B$ and in none of the other sets.

We could have an element like that this that isn't in C, D, E, nor F, and then it won't exist in the set on the right!

Let's make a concrete example showing this

Q7 - Unioned Intersections

give <u>one specific</u> example, don't need to give all times this is true, just one!!

Show that there exists sets A, B, C, D, E, F such that $(A \cap B) \cup (C \cap D) \cup (E \cap F) \not\subseteq (A \cup B) \cap (C \cup D) \cap (E \cup F)$.

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

Q7 - Unioned Intersections

evaluate the set on the left and right side

Show that there exists sets A, B, C, D, E, F such that $(A \cap B) \cup (C \cap D) \cup (E \cap F) \not\subseteq (A \cup B) \cap (C \cup D) \cap (E \cup F)$.

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}. This is the set on the left.

$A \cup B$ is the set {3}, $C \cup D$ is the set {5}, and $E \cup F$ is the set {5}.
There are no overlapping elements between these, so the intersection $(A \cup B) \cap (C \cup D) \cap (E \cup F)$ is the empty set ø. This is the set on the right.

Q7 - Unioned Intersections

we need to show that left is not a subset of right. to *disprove* "for arbitrary x in left, x is in right", we just need to give one counterexample of an element in left that's not in right!

Show that there exists sets A, B, C, D, E, F such that $(A \cap B) \cup (C \cap D) \cup (E \cap F) \not\subseteq (A \cup B) \cap (C \cup D) \cap (E \cup F)$.

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}. This is the set on the left.

$A \cup B$ is the set {3}, $C \cup D$ is the set {5}, and $E \cup F$ is the set {5}.
There are no overlapping elements between these, so the intersection $(A \cup B) \cap (C \cup D) \cap (E \cup F)$ is the empty set ø. This is the set on the right.

Consider x = 3. x is in the set on the left, but not in the set on the right!

Q7 - Unioned Intersections

we need to show that left is <u>not</u> a subset of right. to *disprove* "for arbitrary x in left, x is in right", we just need to give one counterexample of an element in left that's not in right!

Show that there exists sets A, B, C, D, E, F such that $(A \cap B) \cup (C \cap D) \cup (E \cap F) \not\subseteq (A \cup B) \cap (C \cup D) \cap (E \cup F)$.

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}. This is the set on the left.

$A \cup B$ is the set {3}, $C \cup D$ is the set {5}, and $E \cup F$ is the set {5}.
There are no overlapping elements between these, so the intersection $(A \cup B) \cap (C \cup D) \cap (E \cup F)$ is the empty set ø. This is the set on the right.

Consider x = 3. x is in the set on the left, but not in the set on the right!

So, it is not true that all elements in $(A \cap B) \cup (C \cap D) \cup (E \cap F)$ are in $(A \cup B) \cap (C \cup D) \cap (E \cup F)$.

✨done✨

Q7 - Unioned Intersections

Show that there exists sets A, B, C, D, E, F such that $(A \cap B) \cup (C \cap D) \cup (E \cap F) \not\subseteq (A \cup B) \cap (C \cup D) \cap (E \cup F)$.

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}. This is the set on the left.

$A \cup B$ is the set {3}, $C \cup D$ is the set {5}, and $E \cup F$ is the set {5}.
There are no overlapping elements between these, so the intersection $(A \cup B) \cap (C \cup D) \cap (E \cup F)$ is the empty set ø. This is the set on the right.

Consider x = 3. x is in the set on the left, but not in the set on the right!

So, it is not true that all elements in (A ∩ B) ∪ (C ∩ D) ∪ (E ∩ F) are in (A ∪ B) ∩ (C ∪ D) ∩ (E ∪ F).

By definition of subset, we have found sets A, B, C, D, E, F such that (A ∩ B) ∪ (C ∩ D) ∪ (E ∩ F) ⊈ (A ∪ B) ∩ (C ∪ D) ∩ (E ∪ F) which is exactly the claim we are trying to prove.

Problem 8:Complementary Sets

Q8 - Complementary Sets

(a) Write $\overline{A \cup B} \subseteq \overline{A} \cap \overline{B}$ as an English statement including an implication.
(b) Take the contrapositive of the statement in (a).
(c) Write the expression from (b) in set notation.
(d) Write an English proof for the statement in part (c).

Work on this with the people around you and then we'll go over it together!

Q8 - Complementary Sets

(a) Write $\overline{A \cup B} \subseteq \overline{A \cap B}$ as an English statement including an implication.

Definition of subset:
For all x, if x is in $\overline{A \cup B}$, then is is also in $\overline{A \cap B}$

Q8 - Complementary Sets

(a) Write $\overline{A \cup B} \subseteq \overline{A \cap B}$ as an English statement including an implication.

Definition of subset:

For all x, if x is in $\overline{A \cup B}$, then is is also in $\overline{A \cap B}$

Apply definition of complement:

For all x, if x is <u>not</u> in $A \cup B$, then x is also <u>not</u> in $A \cap B$.

Q8 - Complementary Sets

(a) Write $\overline{A \cup B} \subseteq \overline{A \cap B}$ as an English statement including an implication.

For all x, if x is <u>not</u> in $A \cup B$, then x is also <u>not</u> in $A \cap B$.

(b) Take the contrapositive of the statement in (a).

Q8 - Complementary Sets

(a) Write $\overline{A \cup B} \subseteq \overline{A \cap B}$ as an English statement including an implication.

For all x, if x is not in $A \cup B$, then x is also not in $A \cap B$.

(b) Take the contrapositive of the statement in (a).

For all x, if x is in $A \cap B$, then x is also in $A \cup B$.

Q8 - Complementary Sets

(a) Write $\overline{A \cup B} \subseteq \overline{A \cap B}$ as an English statement including an implication.

For all x, if x is not in $A \cup B$, then x is also not in $A \cap B$.

(b) Take the contrapositive of the statement in (a).

For all x, if x is in $A \cap B$, then x is also in $A \cup B$.

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

Q8 - Complementary Sets

(a) Write $\overline{A \cup B} \subseteq \overline{A \cap B}$ as an English statement including an implication.

For all x, if x is not in $A \cup B$, then x is also not in $A \cap B$.

(b) Take the contrapositive of the statement in (a).

For all x, if x is in $A \cap B$, then x is also in $A \cup B$.

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

$A \cap B \subseteq A \cup B$ (*applying definition of subset*)

Q8 - Complementary Sets

(b) For all x, if x is in $A \cap B$, then x is also in $A \cup B$.

(c) $A \cap B \subseteq A \cup B$

(d) Write an English proof for the statement in part (c)

Q8 - Complementary Sets

(b) For all x, if x is in $A \cap B$, then x is also in $A \cup B$.

(c) $A \cap B \subseteq A \cup B$

(d) Write an English proof for the statement in part (c)

Let x be an arbitrary element of $A \cap B$.

Q8 - Complementary Sets

(b) For all x, if x is in $A \cap B$, then x is also in $A \cup B$.

(c) $A \cap B \subseteq A \cup B$

(d) Write an English proof for the statement in part (c)

Let x be an arbitrary element of $A \cap B$.

By def of intersection, this means $x \in A$ and $x \in B$.

Q8 - Complementary Sets

(b) For all x, if x is in $A \cap B$, then x is also in $A \cup B$.

(c) $A \cap B \subseteq A \cup B$

(d) Write an English proof for the statement in part (c)

Let x be an arbitrary element of $A \cap B$.

By def of intersection, this means $x \in A$ and $x \in B$.

Since $x \in A$, we know $x \in A$ or $x \in B$.

Q8 - Complementary Sets

(b) For all x, if x is in $A \cap B$, then x is also in $A \cup B$.

(c) $A \cap B \subseteq A \cup B$

(d) Write an English proof for the statement in part (c)

Let x be an arbitrary element of $A \cap B$.
By def of intersection, this means $x \in A$ and $x \in B$.
Since $x \in A$, we know $x \in A$ or $x \in B$.
By definition of union, $x \in A \cup B$

Q8 - Complementary Sets

(b) For all x, if x is in $A \cap B$, then x is also in $A \cup B$.

(c) $A \cap B \subseteq A \cup B$

(d) Write an English proof for the statement in part (c)

Let x be an arbitrary element of $A \cap B$.

By def of intersection, this means $x \in A$ and $x \in B$.

Since $x \in A$, we know $x \in A$ or $x \in B$.

By definition of union, $x \in A \cup B$

Since x was an arbitrary element of $A \cap B$, we have shown that $A \cap B \subseteq A \cup B$ as require

Q8 - Complementary Sets

(b) For all x, if x is in $A \cap B$, then x is also in $A \cup B$.

(c) $A \cap B \subseteq A \cup B$

(d) Write an English proof for the statement in part (c).

Let x be an arbitrary element of $A \cap B$.
By def of intersection, this means $x \in A$ and $x \in B$.
Since $x \in A$, we know $x \in A$ or $x \in B$.
By definition of union, $x \in A \cup B$
Since x was an arbitrary element of $A \cap B$, we have shown that $A \cap B \subseteq A \cup B$ as required