CSE 311 Section MR

Midterm Review

Administrivia

Announcements & Reminders

- HW5 (BOTH PARTS)
  - BOTH PARTS were due Wednesday 11/8 @ 10pm
  - Late due date Friday 11/10

- Midterm is Coming Next Week!!!
  - Wednesday 10/15 @ 6-7:30 pm in BAG 131 and 154
  - If you cannot make it, please let us know ASAP and we will schedule you for a makeup

Problem 1: Translation

Problem 1 – Translation

Let your domain of discourse be all coffee drinks. You should use the following predicates:

- soy(x) is true iff x contains soy milk.
- whole(x) is true iff x contains whole milk.
- sugar(x) is true iff x contains sugar
- decaf(x) is true iff x is not caffeinated.
- vegan(x) is true iff x is vegan.
- RobbieLikes(x) is true iff Robbie likes the drink x.

Translate each of the following statements into predicate logic. You may use quantifiers, the predicates above, and usual math connectors like = and ≠.

a) Coffee drinks with whole milk are not vegan

b) Robbie only likes one coffee drink, and that drink is not vegan

c) There is a drink that has both sugar and soy milk.

Work on this problem with the people around you.

Problem 1 – Translation

- soy(x) is true iff x contains soy milk
- whole(x) is true iff x contains whole milk
- sugar(x) is true iff x contains sugar
- decaf(x) is true iff x is not caffeinate
- vegan(x) is true iff x is vegan
- RobbieLikes(x) is true iff Robbie likes the drink x

a) Coffee drinks with whole milk are not vegan

b) Robbie only likes one coffee drink, and that drink is not vegan

c) There is a drink that has both sugar and soy milk.

Problem 1 – Translation

- soy(x) is true iff x contains soy milk
- whole(x) is true iff x contains whole milk
- sugar(x) is true iff x contains sugar
- decaf(x) is true iff x is not caffeinate
- vegan(x) is true iff x is vegan
- RobbieLikes(x) is true iff Robbie likes the drink x

a) Coffee drinks with whole milk are not vegan

$$\forall x(\text{whole}(x) \rightarrow \neg\text{vegan}(x))$$

b) Robbie only likes one coffee drink, and that drink is not vegan

c) There is a drink that has both sugar and soy milk.

Problem 1 – Translation

- soy(x) is true iff x contains soy milk
- whole(x) is true iff x contains whole milk
- sugar(x) is true iff x contains sugar
- decaf(x) is true iff x is not caffeinate
- vegan(x) is true iff x is vegan
- RobbieLikes(x) is true iff Robbie likes the drink x

a) Coffee drinks with whole milk are not vegan

$$\forall x(\text{whole}(x) \rightarrow \neg\text{vegan}(x))$$

b) Robbie only likes one coffee drink, and that drink is not vegan

$$\exists x \forall y(\text{RobbieLikes}(x) \land \neg\,\text{Vegan}(x) \land [\text{RobbieLikes}(y) \rightarrow x = y])$$

c) There is a drink that has both sugar and soy milk.

Problem 1 – Translation

- soy(x) is true iff x contains soy milk
- whole(x) is true iff x contains whole milk
- sugar(x) is true iff x contains sugar
- decaf(x) is true iff x is not caffeinate
- vegan(x) is true iff x is vegan
- RobbieLikes(x) is true iff Robbie likes the drink x

a) Coffee drinks with whole milk are not vegan

$\forall x(\text{whole}(x) \rightarrow \neg\text{vegan}(x))$

b) Robbie only likes one coffee drink, and that drink is not vegan

$\exists x\forall y(\text{RobbieLikes}(x) \land \neg\,\text{Vegan}(x) \land [\text{RobbieLikes}(y) \rightarrow x = y])$
Or $\exists x(\text{RobbieLikes}(x) \land \neg\,\text{Vegan}(x) \land \forall y[\text{RobbieLikes}(y) \rightarrow x = y])$

c) There is a drink that has both sugar and soy milk.

Problem 1 – Translation

- soy(x) is true iff x contains soy milk
- whole(x) is true iff x contains whole milk
- sugar(x) is true iff x contains sugar
- decaf(x) is true iff x is not caffeinate
- vegan(x) is true iff x is vegan
- RobbieLikes(x) is true iff Robbie likes the drink x

a) Coffee drinks with whole milk are not vegan

$$\forall x(\text{whole}(x) \rightarrow \neg\text{vegan}(x))$$

b) Robbie only likes one coffee drink, and that drink is not vegan

$$\exists x \forall y(\text{RobbieLikes}(x) \wedge \neg \text{Vegan}(x) \wedge [\text{RobbieLikes}(y) \rightarrow x = y])$$

Or $\exists x(\text{RobbieLikes}(x) \wedge \neg \text{Vegan}(x) \wedge \forall y[\text{RobbieLikes}(y) \rightarrow x = y])$

c) There is a drink that has both sugar and soy milk.

$$\exists x\left(\text{sugar}(x) \wedge \text{soy}(x)\right)$$

Problem 1 – Translation

Let your domain of discourse be all coffee drinks. You should use the following predicates:

- $\text{soy}(x)$ is true iff x contains soy milk.
- $\text{whole}(x)$ is true iff x contains whole milk.
- $\text{sugar}(x)$ is true iff x contains sugar
- $\text{decaf}(x)$ is true iff x is not caffeinated.
- $\text{vegan}(x)$ is true iff x is vegan.
- $\text{RobbieLikes}(x)$ is true iff Robbie likes the drink x.

Translate the following symbolic logic statement into a (natural) English sentence. Take advantage of domain restriction.

$$\forall x([\text{decaf}(x) \wedge \text{RobbieLikes}(x)] \rightarrow \text{sugar}(x))$$

Work on this problem with the people around you.

Problem 1 – Translation

- soy(x) is true iff x contains soy milk
- whole(x) is true iff x contains whole milk
- sugar(x) is true iff x contains sugar
- decaf(x) is true iff x is not caffeinate
- vegan(x) is true iff x is vegan
- RobbieLikes(x) is true iff Robbie likes the drink x

$$\forall x([\text{decaf}(x) \wedge \text{RobbieLikes}(x)] \rightarrow \text{sugar}(x))$$

Problem 1 – Translation

- $\text{soy}(x)$ is true iff x contains soy milk
- $\text{whole}(x)$ is true iff x contains whole milk
- $\text{sugar}(x)$ is true iff x contains sugar
- $\text{decaf}(x)$ is true iff x is not caffeinate
- $\text{vegan}(x)$ is true iff x is vegan
- $\text{RobbieLikes}(x)$ is true iff Robbie likes the drink x

$$\forall x([\text{decaf}(x) \land \text{RobbieLikes}(x)] \rightarrow \text{sugar}(x))$$

Every decaf drink that Robbie likes has sugar.

Problem 1 – Translation

- soy(x) is true iff x contains soy milk
- whole(x) is true iff x contains whole milk
- sugar(x) is true iff x contains sugar
- decaf(x) is true iff x is not caffeinate
- vegan(x) is true iff x is vegan
- RobbieLikes(x) is true iff Robbie likes the drink x

$$\forall x([\text{decaf}(x) \land \text{RobbieLikes}(x)] \rightarrow \text{sugar}(x))$$

Every decaf drink that Robbie likes has sugar.

Statements like "For every decaf drink, if Robbie likes it then it has sugar" are equivalent, but only partially take advantage of domain restriction.

Problem 2: Set Theory

Problem 2 – Set Theory

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

Problem 2 – Set Theory

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

First, translate the claim into predicate logic.

Then, write the proof.

Problem 2 – Set Theory

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

First, translate the claim into predicate logic.

$$\forall X \left[\left((A \subseteq B) \wedge \left(X \in \mathcal{P}(A) \right) \right) \to \left(X \in \mathcal{P}(B) \right) \right]$$

Then, write the proof.

Work on this problem with the people around you.

Problem 2 – Set Theory

$$\forall X\left[\left((A \subseteq B) \wedge \left(X \in \mathcal{P}(A)\right)\right) \rightarrow \left(X \in \mathcal{P}(B)\right)\right]$$

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

Problem 2 – Set Theory

$$\forall X \left[\left((A \subseteq B) \wedge \left(X \in \mathcal{P}(A) \right) \right) \rightarrow \left(X \in \mathcal{P}(B) \right) \right]$$

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

Suppose $A \subseteq B$. Let the set X be an arbitrary element of $\mathcal{P}(A)$, so $X \in \mathcal{P}(A)$.

$\ldots$

Since X was arbitrary in $\mathcal{P}(A)$, we have shown $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

Problem 2 – Set Theory

$$\forall X \left[\left((A \subseteq B) \wedge \left(X \in \mathcal{P}(A)\right)\right) \rightarrow \left(X \in \mathcal{P}(B)\right)\right]$$

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

Suppose $A \subseteq B$. Let the set X be an arbitrary element of $\mathcal{P}(A)$, so $X \in \mathcal{P}(A)$.

Then by definition of powerset, $X \subseteq A$.

$\ldots$

Since X was arbitrary in $\mathcal{P}(A)$, we have shown $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

Problem 2 – Set Theory

$\forall X\left[\left((A \subseteq B) \land \left(X \in \mathcal{P}(A)\right)\right) \to \left(X \in \mathcal{P}(B)\right)\right]$

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

Suppose $A \subseteq B$. Let the set X be an arbitrary element of $\mathcal{P}(A)$, so $X \in \mathcal{P}(A)$.

Then by definition of powerset, $X \subseteq A$.
Let y be an arbitrary element of X, so $y \in X$.
$\ldots$

Since X was arbitrary in $\mathcal{P}(A)$, we have shown $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

Problem 2 – Set Theory

$\forall X\left[\left((A \subseteq B) \wedge (X \in \mathcal{P}(A))\right) \rightarrow (X \in \mathcal{P}(B))\right]$

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

Suppose $A \subseteq B$. Let the set X be an arbitrary element of $\mathcal{P}(A)$, so $X \in \mathcal{P}(A)$.

Then by definition of powerset, $X \subseteq A$.
Let y be an arbitrary element of X, so $y \in X$.
Then since $X \subseteq A$, by definition of subset, $y \in A$.
…

Since X was arbitrary in $\mathcal{P}(A)$, we have shown $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

Problem 2 – Set Theory

$$\forall X\left[\left((A \subseteq B) \wedge (X \in \mathcal{P}(A))\right) \rightarrow (X \in \mathcal{P}(B))\right]$$

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

Suppose $A \subseteq B$. Let the set X be an arbitrary element of $\mathcal{P}(A)$, so $X \in \mathcal{P}(A)$.

Then by definition of powerset, $X \subseteq A$.
Let y be an arbitrary element of X, so $y \in X$.
Then since $X \subseteq A$, by definition of subset, $y \in A$.
Since $A \subseteq B$, by definition of subset again, $y \in B$.
$\ldots$

Since X was arbitrary in $\mathcal{P}(A)$, we have shown $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

Problem 2 – Set Theory

$\forall X\left[\left((A \subseteq B) \wedge \left(X \in \mathcal{P}(A)\right)\right) \to \left(X \in \mathcal{P}(B)\right)\right]$

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

Suppose $A \subseteq B$. Let the set X be an arbitrary element of $\mathcal{P}(A)$, so $X \in \mathcal{P}(A)$.

Then by definition of powerset, $X \subseteq A$.
Let y be an arbitrary element of X, so $y \in X$.
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, $X \subseteq B$.
…

Since X was arbitrary in $\mathcal{P}(A)$, we have shown $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

Problem 2 – Set Theory

$$\forall X\left[\left((A \subseteq B) \wedge (X \in \mathcal{P}(A))\right) \rightarrow (X \in \mathcal{P}(B))\right]$$

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

Suppose $A \subseteq B$. Let the set X be an arbitrary element of $\mathcal{P}(A)$, so $X \in \mathcal{P}(A)$.

Then by definition of powerset, $X \subseteq A$.
Let y be an arbitrary element of X, so $y \in X$.
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 $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

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: $\forall y[\left(y \equiv 1 \pmod{p}\right) \rightarrow \left(y^2 \equiv 1 \pmod{p}\right)]$

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: $\forall y[(y \equiv 1 \pmod{p}) \to (y^2 \equiv 1 \pmod{p})]$

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: $\forall y[\left(y \equiv 1 \pmod{p}\right) \rightarrow \left(y^2 \equiv 1 \pmod{p}\right)]$

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 $y^2 \equiv 1 (\mathrm{mod}\ p)$
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 $x \equiv 1 \pmod{p}$.

$\dots$

$x^2 \equiv 1 \pmod{p}$.
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 $pk = (x - 1)$.

$\ldots$

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

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 $pk(x + 1) = (x - 1)(x + 1)$.
$\dots$

$x^2 \equiv 1 \pmod{p}$.
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 $p(k(x + 1)) = (x - 1)(x + 1)$.
$\dots$

$x^2 \equiv 1 \pmod{p}$.
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
$p(k(x + 1)) = x^2 - 1$

$\ldots$
$x^2 \equiv 1 \pmod{p}$.
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, $p \mid x^2 - 1$.
$\ldots x^2 \equiv 1 \pmod{p}$.
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.

<u>Base Case:</u> $P(0)$: 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.

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

<u>Inductive Step:</u> Goal: Show $P(k+1)$:

<u>Conclusion:</u> 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 $P(k+1)$: $S_{k+1} = \frac{1}{6}(k+1)((k+1)+1)(2(k+1)+1)$

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

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

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

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

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

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

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

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

Problem 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≥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 of 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 of 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 6^{th} 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 of 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 of 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 of 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 of 7. Prove that Robbie can buy exactly n snacks for all integers n≥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.

That’s All, Folks!

Thanks for coming to section this week!
Any questions?