

# CSE 311 Section MR

**Midterm Review**

# Administrivia



# Announcements & Reminders

- HW6
  - Was due Wednesday 11/6
  - Late due date Saturday 11/9
- Midterm is Coming Next Week!!!
  - Wednesday 11/13 @ 6-7:30 pm in PAA A102 and A118
  - 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:

- $\text{soy}(x)$  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 each of the following statements into predicate logic. You may use quantifiers, the predicates above, and usual math connectors like  $=$  and  $\neq$ .

- 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

a) Coffee drinks with whole milk are not vegan

- $\text{soy}(x)$  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  $x$

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

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.

- $\text{soy}(x)$  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  $x$

# 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  $x$

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

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

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



# 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  $x$

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

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

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

# 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  $x$

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

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

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

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

# 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  $x$ .

(a) Coffee drinks with whole milk are not vegan.

(d) Translate the contrapositive of part (a) and write a matching (natural) English sentence.

Work on this problem with the people around you.

# 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  $x$

(a) Coffee drinks with whole milk are not vegan.

(d) Translate the contrapositive of part (a) and write a matching (natural) English sentence.

# 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  $x$

(a) Coffee drinks with whole milk are not vegan.

(d) Translate the contrapositive of part (a) and write a matching (natural) English sentence.

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

# 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  $x$

(a) Coffee drinks with whole milk are not vegan.

(d) Translate the contrapositive of part (a) and write a matching (natural) English sentence.

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

Vegan coffee drinks do not contain whole milk.

# 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

- $\text{soy}(x)$  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  $x$

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



# 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  $x$

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

Every decaf drink that Robbie likes has sugar.

# 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  $x$

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

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 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  $x$ .

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

Write the negation of part (e) in predicate logic and translate it into a (natural) English sentence. Take advantage of domain restriction.

# Problem 1 – Translation

Negate:

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

- $\text{soy}(x)$  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  $x$

# Problem 1 – Translation

Negate:

- $\text{soy}(x)$  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  $x$

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

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

$$\equiv \exists x(\neg([\text{decaf}(x) \wedge \text{RobbieLikes}(x)] \rightarrow \text{sugar}(x)))$$

$$\equiv \exists x(\neg(\neg[\text{decaf}(x) \wedge \text{RobbieLikes}(x)] \vee \text{sugar}(x)))$$

$$\equiv \exists x(\neg\neg[\text{decaf}(x) \wedge \text{RobbieLikes}(x)] \wedge \neg\text{sugar}(x))$$

$$\equiv \exists x(\text{decaf}(x) \wedge \text{RobbieLikes}(x) \wedge \neg\text{sugar}(x))$$

# Problem 1 – Translation

Negate:

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

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

$$\equiv \exists x(\neg([\text{decaf}(x) \wedge \text{RobbieLikes}(x)] \rightarrow \text{sugar}(x)))$$

$$\equiv \exists x(\neg(\neg[\text{decaf}(x) \wedge \text{RobbieLikes}(x)] \vee \text{sugar}(x)))$$

$$\equiv \exists x(\neg\neg[\text{decaf}(x) \wedge \text{RobbieLikes}(x)] \wedge \neg \text{sugar}(x))$$

$$\equiv \exists x(\text{decaf}(x) \wedge \text{RobbieLikes}(x) \wedge \neg \text{sugar}(x))$$

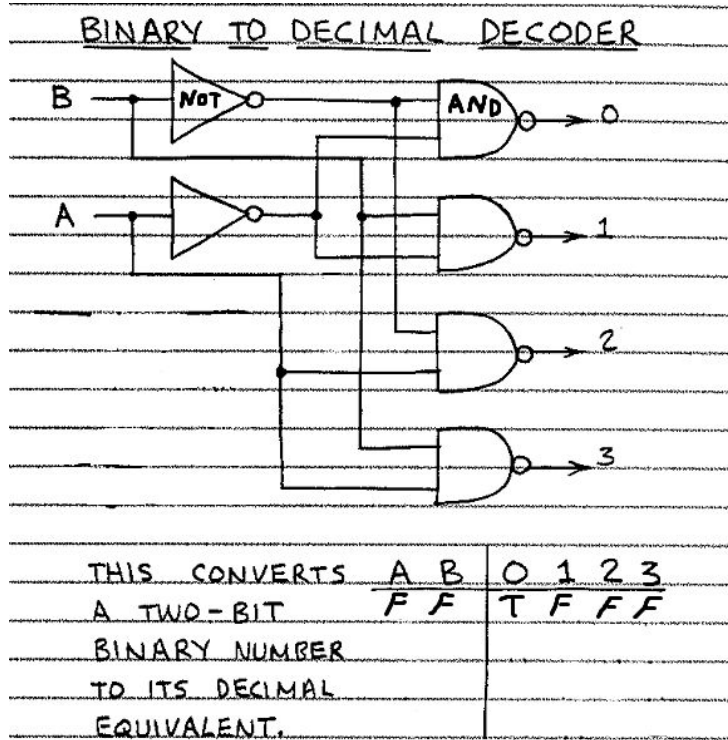
- $\text{soy}(x)$  is true iff  $x$  contains soy milk
- $\text{whole}(x)$  is true iff  $x$  contains whole milk
- $\text{sugar}(x)$  is true iff  $x$  contains sugar
- $\text{decaf}(x)$  is true iff  $x$  is not caffeinate
- $\text{vegan}(x)$  is true iff  $x$  is vegan
- $\text{RobbieLikes}(x)$  is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

There is a decaf drink that  
Robbie likes without sugar.

# Problem 2: Circuits and Normal Forms



## Problem 2 – Circuits and Normal Forms

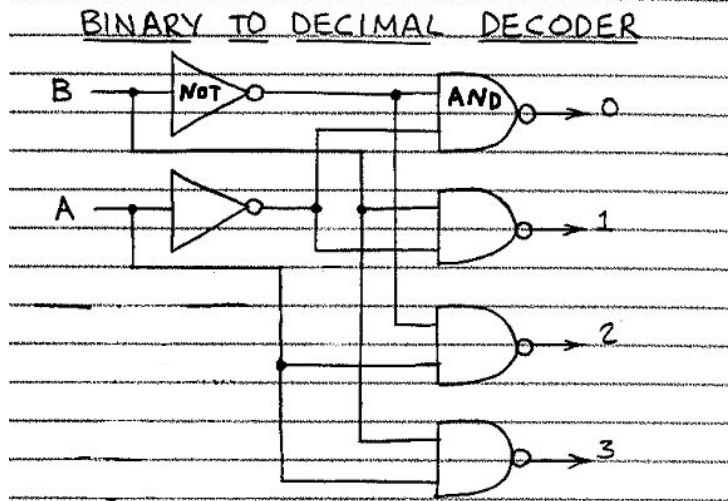


Here's a complex circuit.

- (a) DNF for the output "2"?
- (b) CNF for the output "1"?
- (c) DNF for the outputs greater than "1"?
- (d) How does adding an input affect the outputs?



## Problem 2 – Circuits and Normal Forms

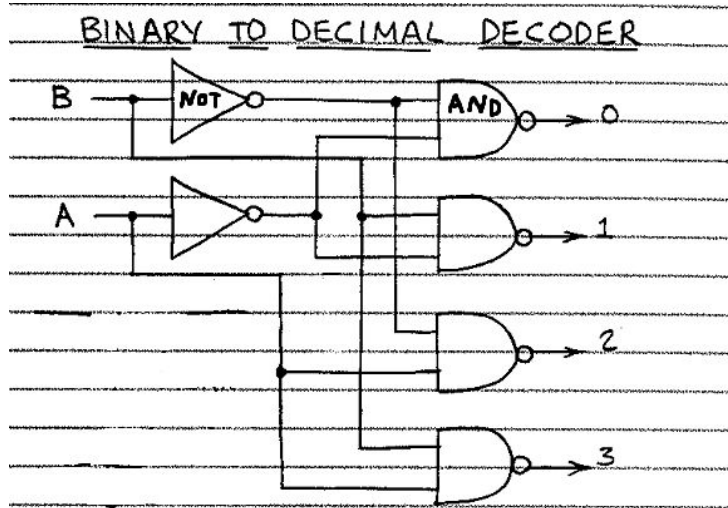


Some tips:

- Complete the truth table
- Focus on one output at a time
- Recall CNF/DNF structure
- Eliminate answers

THIS CONVERTS	A	B	0	1	2	3
A TWO-BIT	F	F	T	F	F	F
BINARY NUMBER						
TO ITS DECIMAL						
EQUIVALENT.						

## Problem 2 – Circuits and Normal Forms



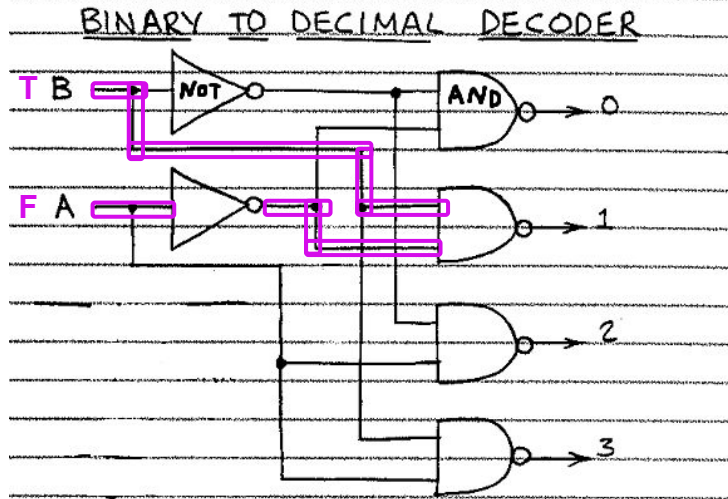
Some tips:

- Complete the truth table
- Focus on one output at a time
- Recall CNF/DNF structure
- Eliminate answers

THIS CONVERTS	A	B	0	1	2	3
A TWO-BIT	F	F	T	F	F	F
BINARY NUMBER						
TO ITS DECIMAL						
EQUIVALENT.						

Work on this problem with the people around you.

## Problem 2 – Circuits and Normal Forms



Some tips:

- Complete the truth table
- Focus on one output at a time
- Recall CNF/DNF structure
- Eliminate answers

*Work backward from one output at a time*

THIS CONVERTS	A	B	0	1	2	3
A TWO-BIT	F	F	T	F	F	F
BINARY NUMBER	F	T	F	T	F	F
TO ITS DECIMAL	T	F	F	F	T	F
EQUIVALENT.	T	T	F	F	F	T

## Problem 2 – Circuits and Normal Forms

(a) What is the DNF for the output “2”?

(i)  $(A \wedge \neg B)$

(ii)  $(A \vee \neg B)$

(iii)  $(\neg A \wedge B) \vee (A \wedge \neg B) \vee (A \wedge B)$

(iv)  $(A \vee B) \wedge (A \vee \neg B) \wedge (\neg A \vee B)$

A	B	0	1	2	3
F	F	T	F	F	F
F	T	F	T	F	F
T	F	F	F	T	F
T	T	F	F	F	T

Some tips:

- Complete the truth table
- Focus on one output at a time
- Recall CNF/DNF structure
- Eliminate answers

*DNF: True rows  $\rightarrow (p \text{ AND } q) \text{ OR } \dots$*

*CNF: False rows  $\rightarrow$  negate  $\rightarrow$*

*(NOT p OR NOT q)  
AND ...*

## Problem 2 – Circuits and Normal Forms

(a) What is the DNF for the output “2”?

(i)  $(A \wedge \neg B)$

~~(ii)  $(A \vee \neg B)$~~

(iii)  $(\neg A \wedge B) \vee (A \wedge \neg B) \vee (A \wedge B)$

~~(iv)  $(A \vee B) \wedge (A \vee \neg B) \wedge (\neg A \vee B)$~~

A	B	0	1	2	3
F	F	T	F	F	F
F	T	F	T	F	F
T	F	F	F	T	F
T	T	F	F	F	T

Some tips:

- Complete the truth table
- Focus on one output at a time
- Recall CNF/DNF structure
- Eliminate answers

*Eliminate based on structure*

## Problem 2 – Circuits and Normal Forms

(a) What is the **DNF** for the output “2”?

(i)  $(A \wedge \neg B)$

~~(ii)  $(A \vee \neg B)$~~

~~(iii)  $(\neg(A \wedge B) \vee (A \wedge \neg B) \vee (A \wedge B))$~~

~~(iv)  $(A \vee B) \wedge (A \vee \neg B) \wedge (\neg A \vee B)$~~

A	B	0	1	2	3
F	F	T	F	F	F
F	T	F	T	F	F
T	F	F	F	T	F
T	T	F	F	F	T

Some tips:

- Complete the truth table
- Focus on one output at a time
- Recall CNF/DNF structure
- **Eliminate answers**

*Eliminate based on number of terms*

## Problem 2 – Circuits and Normal Forms

(a) What is the DNF for the output “2”?

(i)  $(A \wedge \neg B)$

~~(ii)  $(A \vee \neg B)$~~

~~(iii)  $(\neg(A \wedge B) \vee (A \wedge \neg B) \vee (A \wedge B))$~~

~~(iv)  $(A \vee B) \wedge (A \vee \neg B) \wedge (\neg A \vee B)$~~

A	B	0	1	2	3
F	F	T	F	F	F
F	T	F	T	F	F
T	F	F	F	T	F
T	T	F	F	F	T

Some tips:

- Complete the truth table
- Focus on one output at a time
- Recall CNF/DNF structure
- Eliminate answers

*DNF: True rows  $\rightarrow (p \text{ AND } q) \text{ OR } \dots$*

*CNF: False rows  $\rightarrow$  negate  $\rightarrow$*

*(NOT p OR NOT q)  
AND ...*

Work on (b), (c), (d) with the folks around you.

## Problem 2 – Circuits and Normal Forms

(b) What is the CNF for the output “1”?

- (i)  $(A \wedge \neg B)$
- (ii)  $(A \vee \neg B)$
- (iii)  $(\neg A \vee \neg B) \wedge (\neg A \vee B) \wedge (A \vee \neg B)$
- (iv)  $(A \vee B) \wedge (\neg A \vee \neg B) \wedge (\neg A \vee B)$

A	B	0	1	2	3
F	F	T	F	F	F
F	T	F	T	F	F
T	F	F	F	T	F
T	T	F	F	F	T

Some tips:

- Complete the truth table
- Focus on one output at a time
- Recall CNF/DNF structure
- Eliminate answers

*DNF: True rows  $\rightarrow (p \text{ AND } q) \text{ OR } \dots$*

*CNF: False rows  $\rightarrow$  negate  $\rightarrow$   
(NOT  $p$  OR NOT  $q$ )  
AND ...*



## Problem 2 – Circuits and Normal Forms

(b) What is the CNF for the output “1”?

~~(i)  $(A \wedge \neg B)$~~

(ii)  $(A \vee \neg B)$

(iii)  $(\neg A \vee \neg B) \wedge (\neg A \vee B) \wedge (A \vee \neg B)$

(iv)  $(A \vee B) \wedge (\neg A \vee \neg B) \wedge (\neg A \vee B)$

A	B	0	1	2	3
F	F	T	F	F	F
F	T	F	T	F	F
T	F	F	F	T	F
T	T	F	F	F	T

Some tips:

- Complete the truth table
- Focus on one output at a time
- Recall CNF/DNF structure
- Eliminate answers

*DNF: True rows  $\rightarrow (p \text{ AND } q) \text{ OR } \dots$*

*CNF: False rows  $\rightarrow$  negate  $\rightarrow$*

*(NOT p OR NOT q)  
AND ...*

## Problem 2 – Circuits and Normal Forms

(b) What is the **CNF** for the output **"1"**?

~~(i)  $(A \wedge B)$~~

(ii)  $(A \vee \neg B)$

(iii)  $(\neg A \vee \neg B) \wedge (\neg A \vee B) \wedge (A \vee \neg B)$

(iv)  $(A \vee B) \wedge (\neg A \vee \neg B) \wedge (\neg A \vee B)$

A	B	0	1	2	3
F	F	T	F	F	F
F	T	F	T	F	F
T	F	F	F	T	F
T	T	F	F	F	T

Some tips:

- Complete the truth table
- Focus on one output at a time
- Recall CNF/DNF structure
- Eliminate answers

*DNF: True rows  $\rightarrow (p \text{ AND } q) \text{ OR } \dots$*

*CNF: False rows  $\rightarrow$  negate  $\rightarrow$*

*(NOT p OR NOT q)  
AND ...*

## Problem 2 – Circuits and Normal Forms

(b) What is the CNF for the output “1”?

~~(i)  $(A \wedge B)$~~

~~(ii)  $(A \vee \neg B)$~~

(iii)  $(\neg A \vee \neg B) \wedge (\neg A \vee B) \wedge (A \vee \neg B)$

(iv)  $(A \vee B) \wedge (\neg A \vee \neg B) \wedge (\neg A \vee B)$

Some tips:

- Complete the truth table
- Focus on one output at a time
- Recall CNF/DNF structure
- Eliminate answers

A	B	0	1	2	3
F	F	T	F	F	F
F	T	F	T	F	F
T	F	F	F	T	F
T	T	F	F	F	T

*CNF is a lot longer than DNF for one element of this circuit...*

## Problem 2 – Circuits and Normal Forms

(c) What is the DNF for the outputs greater than “1”?

A	B	0	1	2	3
F	F	T	F	F	F
F	T	F	T	F	F
T	F	F	F	T	F
T	T	F	F	F	T

Some tips:

- Complete the truth table
- Focus on one output at a time
- Recall CNF/DNF structure
- Eliminate answers

*DNF: True rows  $\rightarrow (p \text{ AND } q) \text{ OR } \dots$*

*CNF: False rows  $\rightarrow$  negate  $\rightarrow$   
(NOT  $p$  OR NOT  $q$ )  
AND ...*

## Problem 2 – Circuits and Normal Forms

(c) What is the DNF for the outputs greater than “1”?

A	B	0	1	2	3
F	F	T	F	F	F
F	T	F	T	F	F
T	F	F	F	T	F
T	T	F	F	F	T

Some tips:

- Complete the truth table
- Focus on one output at a time
- Recall CNF/DNF structure
- Eliminate answers

*DNF: True rows  $\rightarrow (p \text{ AND } q) \text{ OR } \dots$*

*CNF: False rows  $\rightarrow$  negate  $\rightarrow$*

*(NOT  $p$  OR NOT  $q$ )  
AND ...*

## Problem 2 – Circuits and Normal Forms

(c) What is the DNF for the outputs greater than “1”?

$$(A \wedge \neg B) \vee (A \wedge B)$$

A	B	0	1	2	3
F	F	T	F	F	F
F	T	F	T	F	F
T	F	F	F	T	F
T	T	F	F	F	T

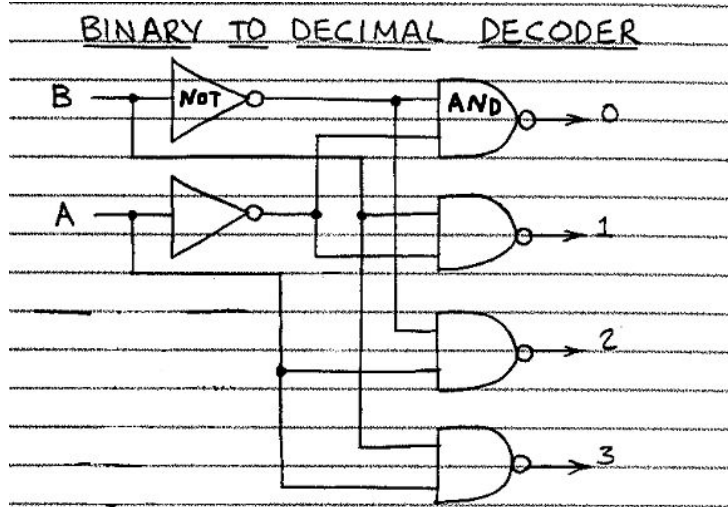
Some tips:

- Complete the truth table
- Focus on one output at a time
- Recall CNF/DNF structure
- Eliminate answers

*For two elements, DNF and CNF are equal length (half of the inputs).*

*1 input combination : 1 output*

## Problem 2 – Circuits and Normal Forms



Some tips:

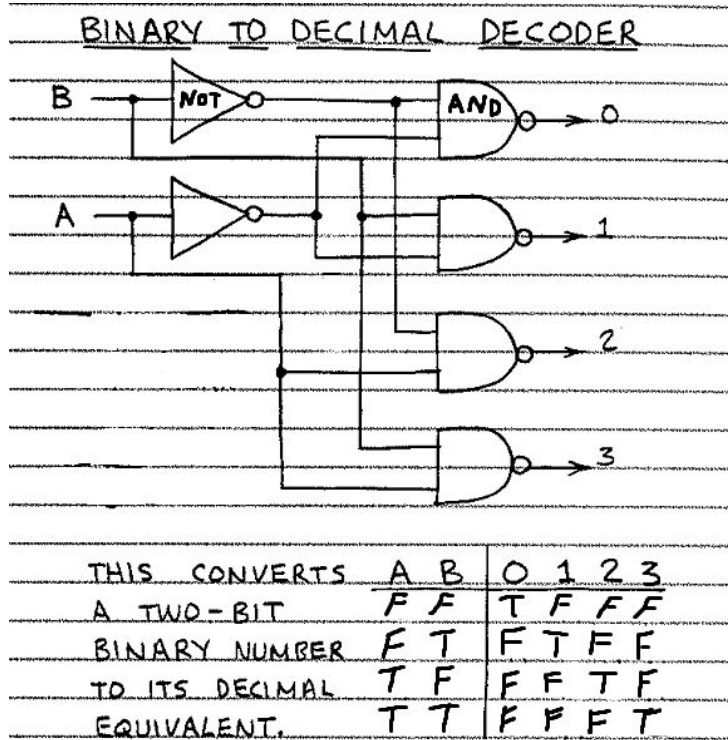
- Complete the truth table
- Focus on one output at a time
- Recall CNF/DNF structure
- Eliminate answers

THIS CONVERTS	A	B	0	1	2	3
A TWO-BIT	F	F	T	F	F	F
BINARY NUMBER	F	T	F	T	F	F
TO ITS DECIMAL	T	F	F	F	T	F
EQUIVALENT.	T	T	F	F	F	T

(d): *Binary*  $\rightarrow$  *Decimal*,  $n \rightarrow 2^n$

*Similar to a truth table! 1:1*

# Problem 2 – Circuits and Normal Forms



Some tips:

- Complete the truth table
- Focus on one output at a time
- Recall CNF/DNF structure
- Eliminate answers

*Complex circuits decomposition,  
implementation in hardware  
(Minecraft redstone)*



Credit:

<https://gaming.stackexchange.com/questions/142191/how-to-build-a-two-bit-binary-to-decimal-decoder-using-redstone>



# Problem 3: Boolean Algebra



## Problem 3 – Boolean Algebra

Consider the following Boolean expression:

$$(A + A' \cdot B) \cdot (A + B)$$

- (a) Simplify the given Boolean expression
- (b) Identify whether the simplified expression is a tautology, contradiction, or neither

Work on this problem with the people around you.

## Problem 3 – Boolean Algebra

Consider the following Boolean expression:

$$(A + A' \cdot B) \cdot (A + B)$$

(a) Simplify the given Boolean expression

(i) Apply the Distributive Law

$$= (A \cdot (A + B)) + (A' \cdot B \cdot (A + B))$$

# Problem 3 – Boolean Algebra

Consider the following Boolean expression:

$$(A + A' \cdot B) \cdot (A + B)$$

(a) Simplify the given Boolean expression

(i) Apply the Distributive Law

$$= (A \cdot (A + B)) + (A' \cdot B \cdot (A + B))$$

(ii) Simplify using the Distributive Law

$$= (A \cdot A + A \cdot B) + (A' \cdot B \cdot A + A' \cdot B \cdot B)$$

## Problem 3 – Boolean Algebra

Consider the following Boolean expression:

$$(A + A' \cdot B) \cdot (A + B)$$

(a) Simplify the given Boolean expression

(iii) Continue simplifying

$$= (A \cdot A + A \cdot B) + (A' \cdot A \cdot B + A' \cdot B \cdot B)$$

$$= (A + A \cdot B) + (0 \cdot B + A' \cdot B)$$

$$= A \cdot (1 + B) + (A' \cdot B)$$

$$= (A \cdot 1) + (A' \cdot B)$$

$$= (A) + (A' \cdot B)$$

## Problem 3 – Boolean Algebra

$$\boxed{(A) + (A' \cdot B)}$$

(b) Identify whether the simplified expression is a tautology, contradiction, or neither

Tautology = always true

Contradiction = always false

Consider  $A = 0$  and  $B = 0$ :

$$\begin{aligned} &= (A) + (A' \cdot B) \\ &= (0) + (0' \cdot 0) \\ &= (0) + (1 \cdot 0) \\ &= (0) + (0) \\ &= 0 \end{aligned}$$

## Problem 3 – Boolean Algebra

$$\boxed{(A) + (A' \cdot B)}$$

(b) Identify whether the simplified expression is a tautology, contradiction, or neither

Tautology = always true

Contradiction = always false

Consider  $A = 1$  and  $B = 0$

$$\begin{aligned} &= (A) + (A' \cdot B) \\ &= (1) + (1' \cdot 0) \\ &= (1) + (0 \cdot 0) \\ &= (1) + (0) \\ &= 1 \end{aligned}$$

## Problem 3 – Boolean Algebra

$$\boxed{(A) + (A' \cdot B)}$$

(b) Identify whether the simplified expression is a tautology, contradiction, or neither

Tautology = always true

Contradiction = always false

Consider  $A = 0$  and  $B = 1$

$$\begin{aligned} &= (A) + (A' \cdot B) \\ &= (0) + (0' \cdot 1) \\ &= (0) + (1 \cdot 1) \\ &= (0) + (1) \\ &= 1 \end{aligned}$$



## Problem 3 – Boolean Algebra

$$\boxed{(A) + (A' \cdot B)}$$

(b) Identify whether the simplified expression is a tautology, contradiction, or neither

Tautology = always true

Contradiction = always false

Consider  $A = 1$  and  $B = 1$

$$\begin{aligned} &= (A) + (A' \cdot B) \\ &= (1) + (1' \cdot 1) \\ &= (1) + (0 \cdot 1) \\ &= (1) + (0) \\ &= 1 \end{aligned}$$

# Problem 3 – Boolean Algebra

$$(A) + (A' \cdot B)$$

(b) Identify whether the simplified expression is a tautology, contradiction, or neither

Tautology = always true

Contradiction = always false

A	B	$(A) + (A' \cdot B)$
0	0	0
1	0	1
0	1	1
1	1	1

Since the expression evaluates to 1 in some cases and 0 in others, it is **neither** a tautology nor a contradiction.

# Problem 4: Even Steven



## Problem 4 – Even Steven

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

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

- (a) Let your domain be integers. Write the predicate logic of this claim.
  
  
  
  
  
  
  
  
  
  
- (b) Write an English proof for this claim.

## Problem 4 – Even Steven

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

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

- (a) Let your domain be integers. Write the predicate logic of this claim.

$$\forall k(\text{Even}(k(k + 3)))$$

- (b) Write an English proof for this claim.

# Problem 4 – Even Steven

(b) Write an English proof for this claim.

Let  $k$  be an arbitrary integer.

**Case 1:  $k$  is even**

**Case 2:  $k$  is odd**

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

# Problem 4 – Even Steven

(b) Write an English proof for this claim.

Let  $k$  be an arbitrary integer.

**Case 1:  $k$  is even**

By the definition of even,  $k = 2j$  for some integer  $j$

So substituting for  $k$  into  $k(k + 3)$ :

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

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

So, by definition of even,  $k(k + 3)$  is even.

**Case 2:  $k$  is odd**

These cases are exhaustive, so the claim that  $k(k + 3)$  is even must hold.

Since  $k$  was arbitrary, the claim holds for all  $k$ .

# Problem 4 – Even Steven

(b) Write an English proof for this claim.

Let  $k$  be an arbitrary integer.

**Case 1:  $k$  is even**

**Case 2:  $k$  is odd**

By the definition of odd,  $k = 2j + 1$  for some integer  $j$ .

So substituting for  $k$  into  $k(k+3)$ :

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

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

So, by definition of even,  $k(k+3)$  is even.

**These cases are exhaustive, so the claim that  $k(k+3)$  is even must hold.**

Since  $k$  was arbitrary, the claim holds for all  $k$ .



# Problem 5: Number Theory



## Problem 5 – 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 use 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 5 – 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 5 – 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 5 – 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 5 – 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  $y^2 \equiv 1^2 \pmod{p}$ .

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

Since  $y$  is arbitrary, the claim holds.

# Problem 5 – 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 5 – 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 5 – 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 5 – 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 5 – 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 5 – 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 5 – 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 5 – 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,  $p \mid x^2 - 1$ .

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

Since  $x$  was arbitrary, the claim holds.

# Problem 5 – 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 5 – 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 use the following theorem without proof: if  $p$  is prime and  $p \mid (ab)$  then  $p \mid a$  or  $p \mid b$ .



# Problem 5 – 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 use 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 5 – 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 use 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 5 – 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 use 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 5 – 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 use 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 5 – 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 use 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  $p \mid (x + 1)$ .

...  $x \equiv 1 \pmod{p}$  or  $x \equiv -1 \pmod{p}$ .

Since  $x$  was arbitrary, the claim holds.

# Problem 5 – 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 use 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 6: Induction



## Problem 6 – 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 6 – 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 6 – 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 6 – 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 6 – Induction

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

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 6 – Induction

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

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 6 – Induction

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

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

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

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

# Problem 6 – Induction

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

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

$$S_{k+1} = 1^2 + 2^2 + \dots + k^2 + (k+1)^2 \quad \text{by definition of } S_n$$

$$= \dots$$

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

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

# Problem 6 – Induction

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

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

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

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



# Problem 6 – Induction

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

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

$$S_{k+1} = 1^2 + 2^2 + \dots + k^2 + (k+1)^2 \quad \text{by definition of } S_n$$

$$= (1^2 + 2^2 + \dots + k^2) + (k+1)^2$$

$$= S_k + (k+1)^2 \quad \text{by definition of } S_n$$

$$= \dots$$

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

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

# Problem 6 – Induction

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

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

$$S_{k+1} = 1^2 + 2^2 + \dots + k^2 + (k+1)^2 \quad \text{by definition of } S_n$$

$$= (1^2 + 2^2 + \dots + k^2) + (k+1)^2$$

$$= S_k + (k+1)^2 \quad \text{by definition of } S_n$$

$$= \frac{1}{6}k(k+1)(2k+1) + (k+1)^2 \quad \text{by I.H.}$$

$$= \dots$$

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

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

# Problem 6 – Induction

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

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

$$S_{k+1} = 1^2 + 2^2 + \dots + k^2 + (k+1)^2 \quad \text{by definition of } S_n$$

$$= (1^2 + 2^2 + \dots + k^2) + (k+1)^2$$

$$= S_k + (k+1)^2 \quad \text{by definition of } S_n$$

$$= \frac{1}{6}k(k+1)(2k+1) + (k+1)^2 \quad \text{by I.H.}$$

$$= (k+1)\left(\frac{1}{6}k(2k+1) + (k+1)\right)$$

$$= \dots$$

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

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

# Problem 6 – Induction

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

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

$$S_{k+1} = 1^2 + 2^2 + \dots + k^2 + (k+1)^2 \quad \text{by definition of } S_n$$

$$= (1^2 + 2^2 + \dots + k^2) + (k+1)^2$$

$$= S_k + (k+1)^2 \quad \text{by definition of } S_n$$

$$= \frac{1}{6}k(k+1)(2k+1) + (k+1)^2 \quad \text{by I.H.}$$

$$= (k+1)\left(\frac{1}{6}k(2k+1) + (k+1)\right)$$

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

$$= \dots$$

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

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

# Problem 6 – Induction

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

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

$$S_{k+1} = 1^2 + 2^2 + \dots + k^2 + (k+1)^2 \quad \text{by definition of } S_n$$

$$= (1^2 + 2^2 + \dots + k^2) + (k+1)^2$$

$$= S_k + (k+1)^2 \quad \text{by definition of } S_n$$

$$= \frac{1}{6}k(k+1)(2k+1) + (k+1)^2 \quad \text{by I.H.}$$

$$= (k+1)\left(\frac{1}{6}k(2k+1) + (k+1)\right)$$

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

$$= \frac{1}{6}(k+1)(2k^2 + k + 6k + 6)$$

$$= \dots$$

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

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

# Problem 6 – Induction

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

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

$$S_{k+1} = 1^2 + 2^2 + \dots + k^2 + (k+1)^2 \quad \text{by definition of } S_n$$

$$= (1^2 + 2^2 + \dots + k^2) + (k+1)^2$$

$$= S_k + (k+1)^2 \quad \text{by definition of } S_n$$

$$= \frac{1}{6}k(k+1)(2k+1) + (k+1)^2 \quad \text{by I.H.}$$

$$= (k+1)\left(\frac{1}{6}k(2k+1) + (k+1)\right)$$

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

$$= \frac{1}{6}(k+1)(2k^2 + k + 6k + 6)$$

$$= \frac{1}{6}(k+1)(2k^2 + 7k + 6)$$

$$= \dots$$

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

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

# Problem 6 – Induction

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

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

$$S_{k+1} = 1^2 + 2^2 + \dots + k^2 + (k+1)^2 \quad \text{by definition of } S_n$$

$$= (1^2 + 2^2 + \dots + k^2) + (k+1)^2$$

$$= S_k + (k+1)^2 \quad \text{by definition of } S_n$$

$$= \frac{1}{6}k(k+1)(2k+1) + (k+1)^2 \quad \text{by I.H.}$$

$$= (k+1)\left(\frac{1}{6}k(2k+1) + (k+1)\right)$$

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

$$= \frac{1}{6}(k+1)(2k^2 + k + 6k + 6)$$

$$= \frac{1}{6}(k+1)(2k^2 + 7k + 6)$$

$$= \frac{1}{6}(k+1)(k+2)(2k+3)$$

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

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

# Problem 7: Strong Induction





## Problem 7 – 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 7 – 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 7 – 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 7 – 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<sup>th</sup> case can be reached by adding 5 to the minimum base case

# Problem 7 – 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 7 – 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  $P(24) \wedge P(25) \wedge \dots \wedge P(k)$  hold for an arbitrary  $k \geq 28$ .

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

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

# Problem 7 – 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  $P(24) \wedge P(25) \wedge \dots \wedge P(k)$  hold for an arbitrary  $k \geq 28$ .

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 7 – 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  $P(24) \wedge P(25) \wedge \dots \wedge P(k)$  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 8: Wait, That Doesn't Add Up



# Problem 8 - Wait, That Doesn't Add Up

Write a proof by contradiction for the following proposition: There exist no integers  $x$  and  $y$  such that  $18x + 6y = 1$ . In predicate logic this could be expressed as  $\forall x \forall y (18x + 6y \neq 1)$ . HINT: Try negating this statement before writing your proof.

Work on this problem with the people around you.

# Problem 8 - Wait, That Doesn't Add Up

Write a proof by contradiction for the following proposition: There exist no integers  $x$  and  $y$  such that  $18x + 6y = 1$ . In predicate logic this could be expressed as  $\forall x \forall y (18x + 6y \neq 1)$ . HINT: Try negating this statement before writing your proof.

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

# Problem 8 - Wait, That Doesn't Add Up

Write a proof by contradiction for the following proposition: There exist no integers  $x$  and  $y$  such that  $18x + 6y = 1$ . In predicate logic this could be expressed as  $\forall x \forall y (18x + 6y \neq 1)$ . HINT: Try negating this statement before writing your proof.

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

$$18x + 6y = 1$$

# Problem 8 - Wait, That Doesn't Add Up

Write a proof by contradiction for the following proposition: There exist no integers  $x$  and  $y$  such that  $18x + 6y = 1$ . In predicate logic this could be expressed as  $\forall x \forall y (18x + 6y \neq 1)$ . HINT: Try negating this statement before writing your proof.

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

$$18x + 6y = 1$$

$$3x + y = \frac{1}{6} \quad \text{Dividing by 6}$$

# Problem 8 - Wait, That Doesn't Add Up

Write a proof by contradiction for the following proposition: There exist no integers  $x$  and  $y$  such that  $18x + 6y = 1$ . In predicate logic this could be expressed as  $\forall x \forall y (18x + 6y \neq 1)$ . HINT: Try negating this statement before writing your proof.

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

$$18x + 6y = 1$$

$$3x + y = \frac{1}{6} \quad \text{Dividing by 6}$$

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

# Problem 9: How Many Elements?



# Problem 9 - How Many Elements?

## 9. How Many Elements?

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

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

(b)  $B = \{\{\}, \{\{\}\}, \{\{\}, \{\}\}, \{\{\}, \{\}, \{\}\}, \dots\}$

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

(d)  $D = \emptyset$

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

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

Work on this problem with the people around you.



# Problem 9 - How Many Elements?

## 9. How Many Elements?

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

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

3

# Problem 9 - How Many Elements?

## 9. How Many Elements?

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

$$(b) \ B = \{\{\}, \{\{\}\}, \{\{\}, \{\}\}, \{\{\}, \{\}, \{\}\}, \dots\}$$

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

So, there are two elements in  $B$ .

# Problem 9 - How Many Elements?

## 9. How Many Elements?

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

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

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

# Problem 9 - How Many Elements?

## 9. How Many Elements?

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

(d)  $D = \emptyset$

0.

# Problem 9 - How Many Elements?

## 9. How Many Elements?

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

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

1.

# Problem 9 - How Many Elements?

## 9. How Many Elements?

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

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

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

## Problem 10: Set = Set



## Problem 10 - Set = Set

Prove the following set identities. Write both a formal inference proof **and** an English proof.

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

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

Work on this problem with the people around you.



## Problem 10 - Set = Set

Prove the following set identities. Write both a formal inference proof **and** an English proof.

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

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

## Problem 10 - Set = Set

Prove the following set identities. Write both a formal inference proof **and** an English proof.

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

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

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

# Problem 11: Set Equality



## Problem 11 - Set Equality

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

Work on this problem with the people around you.

## Problem 11 - Set Equality

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

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

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

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

# **That's All, Folks!**

**Thanks for coming to section this week!**  
**Any questions?**