CS103
Winter 2025

Lecture 02:

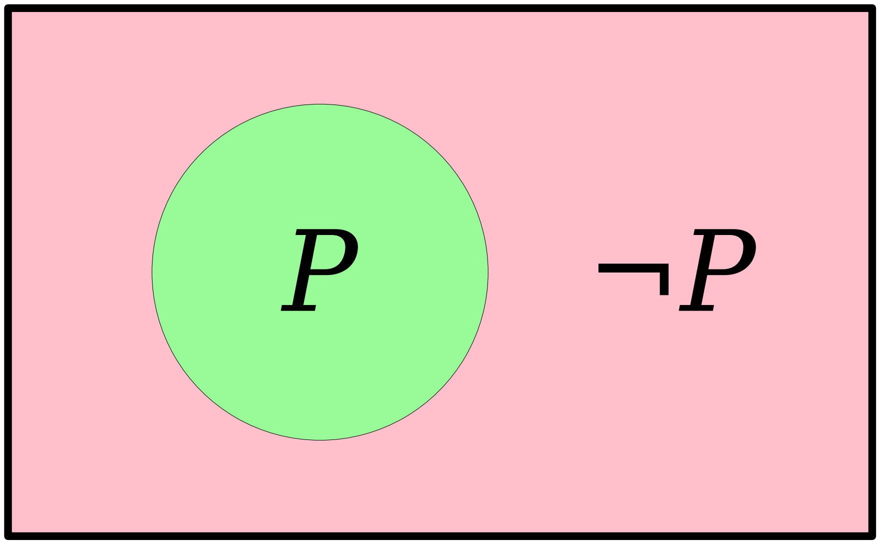
Indirect Proofs

CS103
Winter 2025

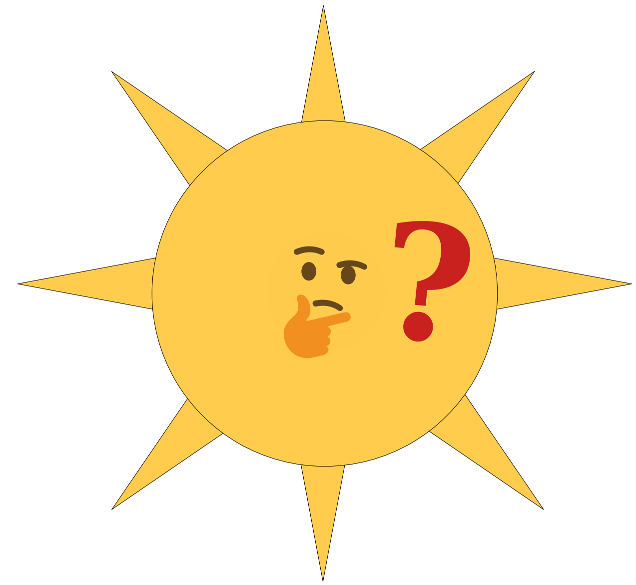
Lecture 02:

Indirect Proofs

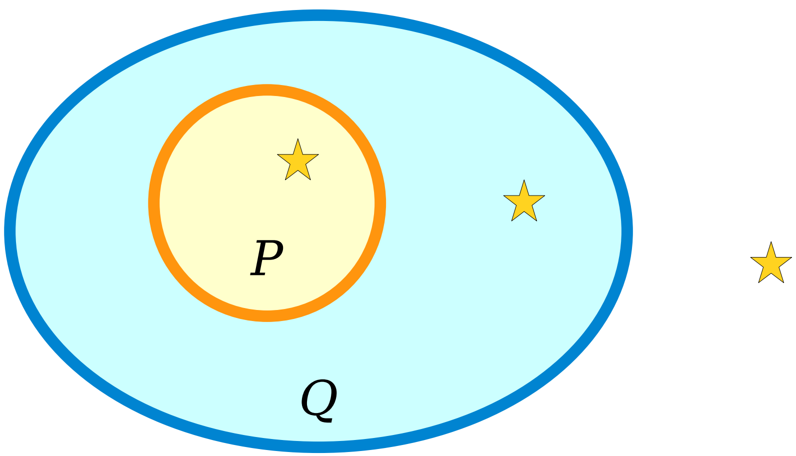
A Story in Four Acts



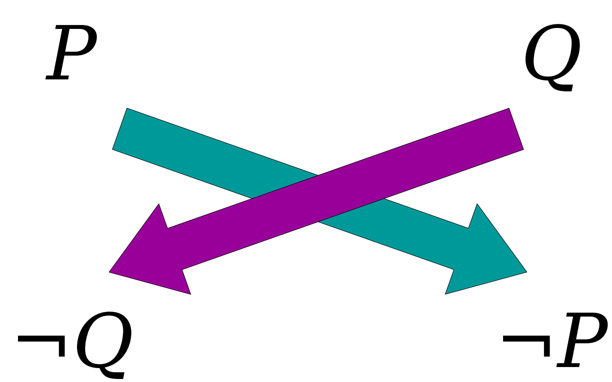
Logical Negation



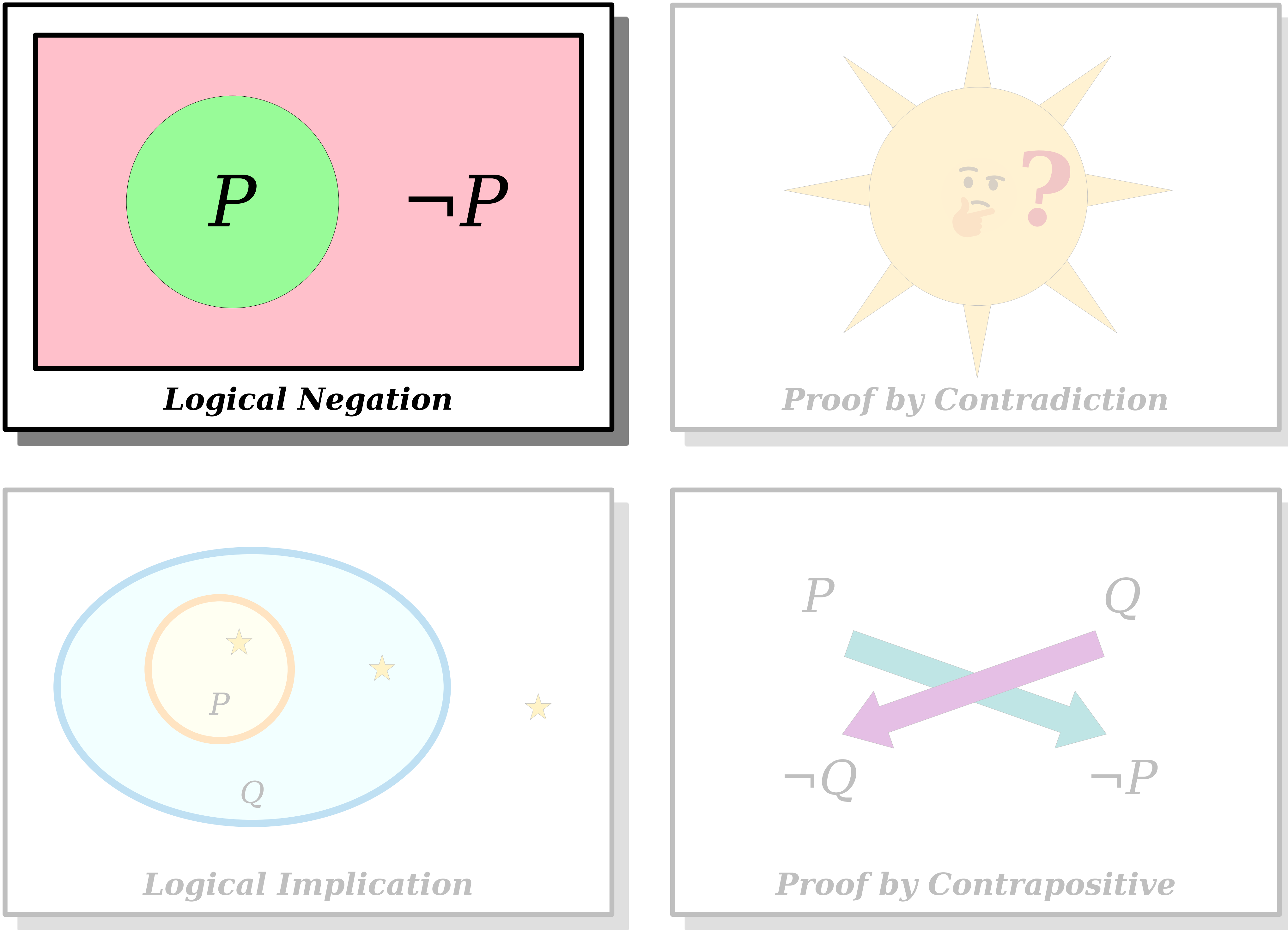
Proof by Contradiction



Logical Implication



Proof by Contrapositive


P
¬P
Logical Negation
?
Proof by Contradiction
P
Q
Logical Implication
P
Q
¬Q
¬P
Proof by Contrapositive

Act I

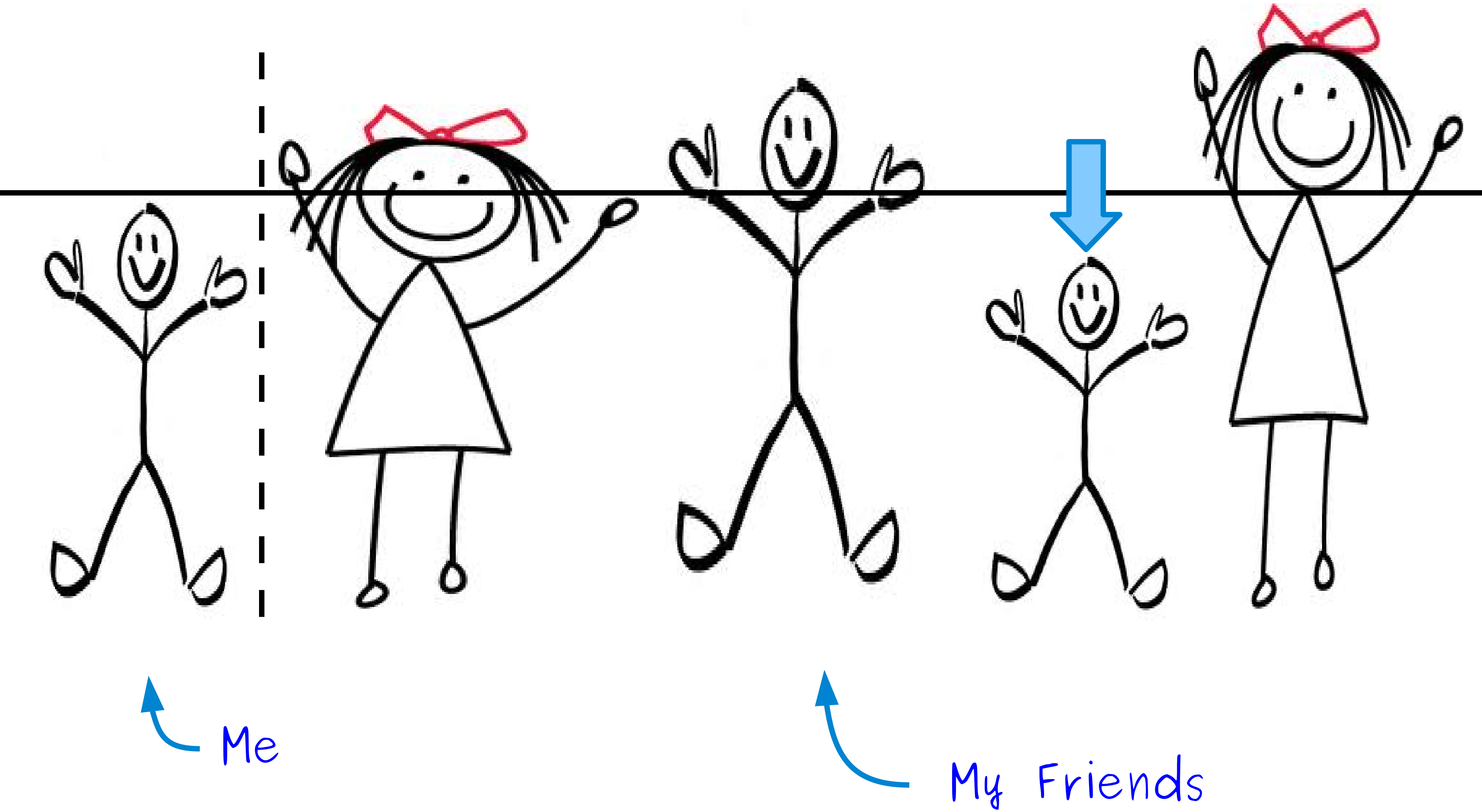
Logical Negation

Negations

- A ***proposition*** is a statement that is either true or false.
- Some examples:
  - If n is an even integer, then n^2 is an even integer.
  - $\emptyset = \mathbb{R}$.
- The ***negation*** of a proposition X is a proposition that is true when X is false and is false when X is true.
- For example, consider the proposition "it is snowing outside."
  - Its negation is "it is not snowing outside."
  - Its negation is *not* "it is sunny outside."
  - Its negation is *not* "we're in the Bay Area."

How do you find the negation of a statement?

“All My Friends Are Taller Than Me”



The negation of the ***universal*** statement

Every *P* is a *Q*

is the ***existential*** statement

There is a *P* that is not a *Q*.

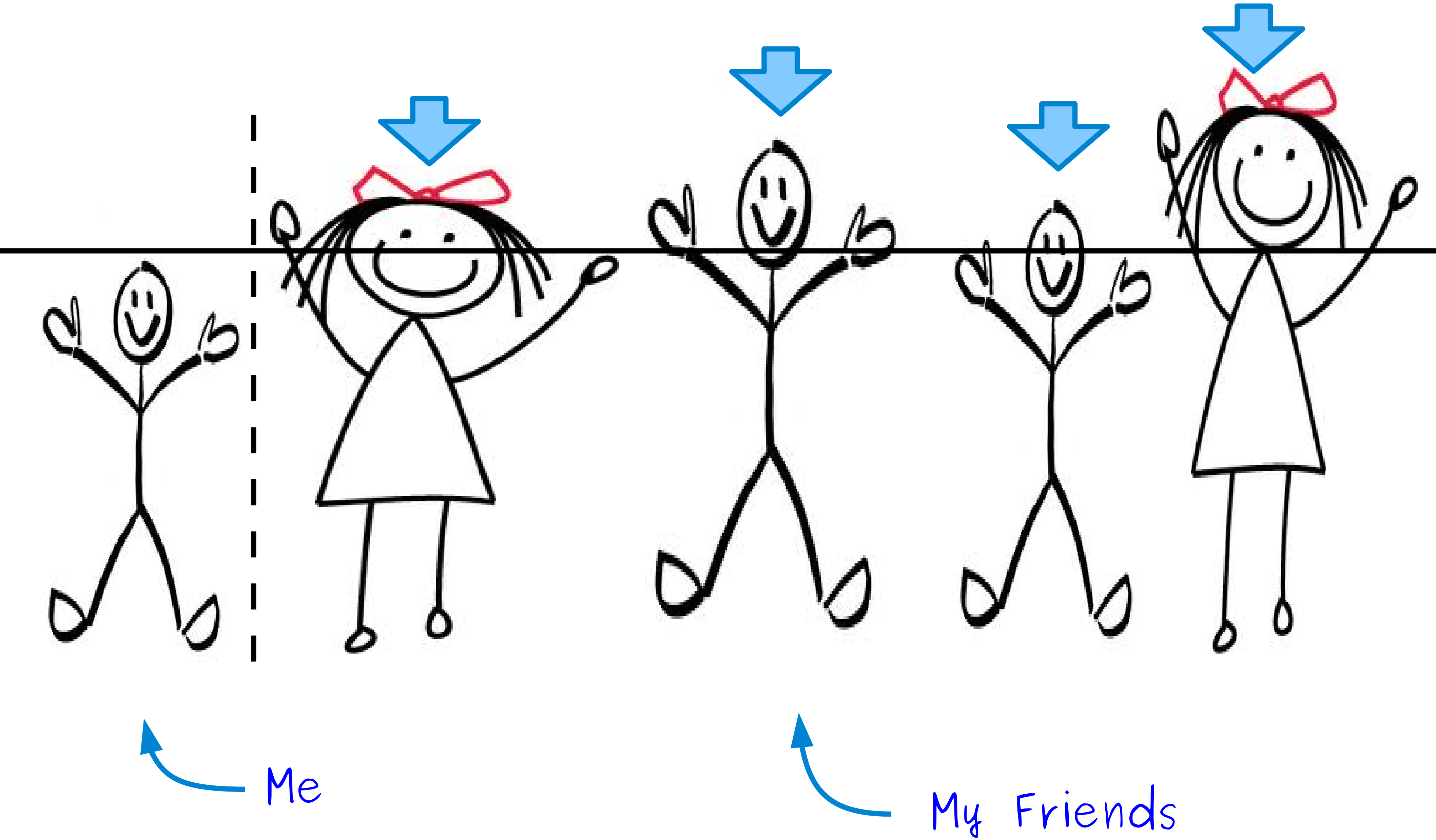
The negation of the ***universal*** statement

For all *x*, *P*(*x*) is true.

is the ***existential*** statement

There exists an *x* where *P*(*x*) is false.

“Some Friend Is Shorter Than Me”



The negation of the ***existential*** statement

There exists a *P* that is a *Q*

is the ***universal*** statement

Every *P* is not a *Q*.

The negation of the ***existential*** statement

There exists an *x* where *P*(*x*) is true

is the ***universal*** statement

For all *x*, *P*(*x*) is false.

Your Turn!

- What’s the negation of the following statement?

“Every brown dog loves every orange cat.”

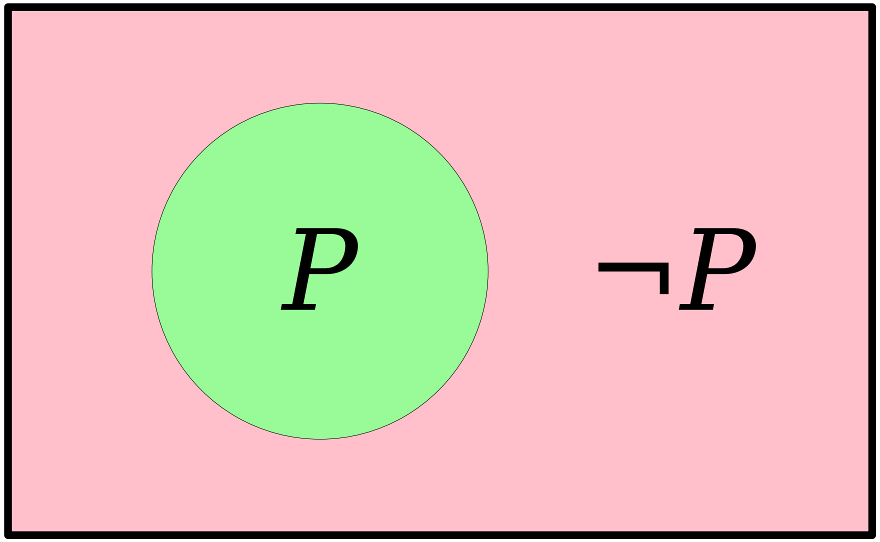
Your Turn!

- What’s the negation of the following statement?

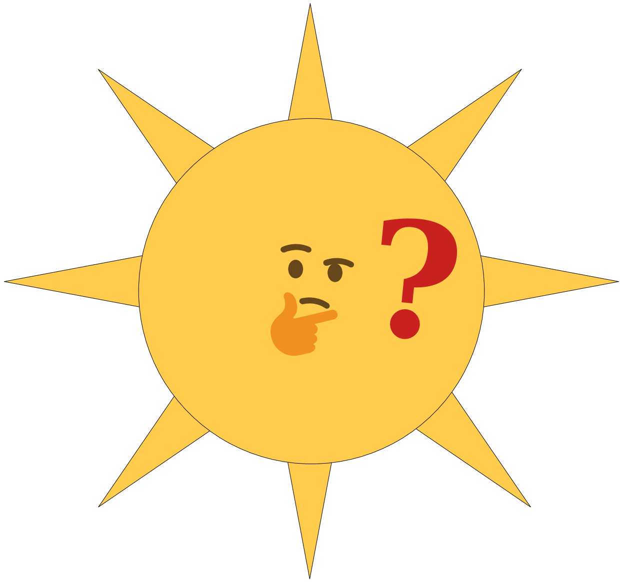
*“**Every brown dog loves every orange cat.**”*

- Answer:

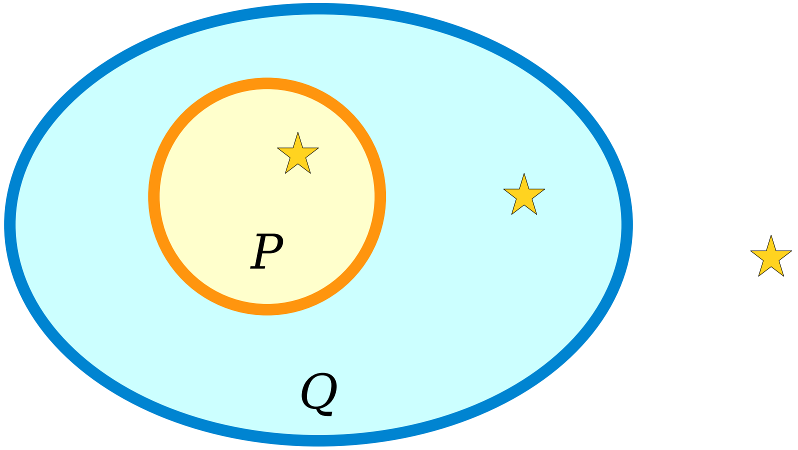
*“**There is a brown dog that doesn’t love some orange cat**”*



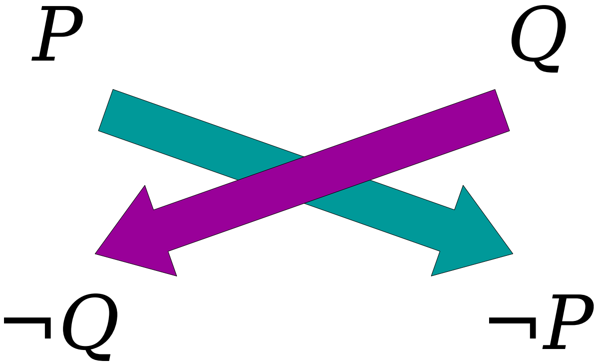
Logical Negation



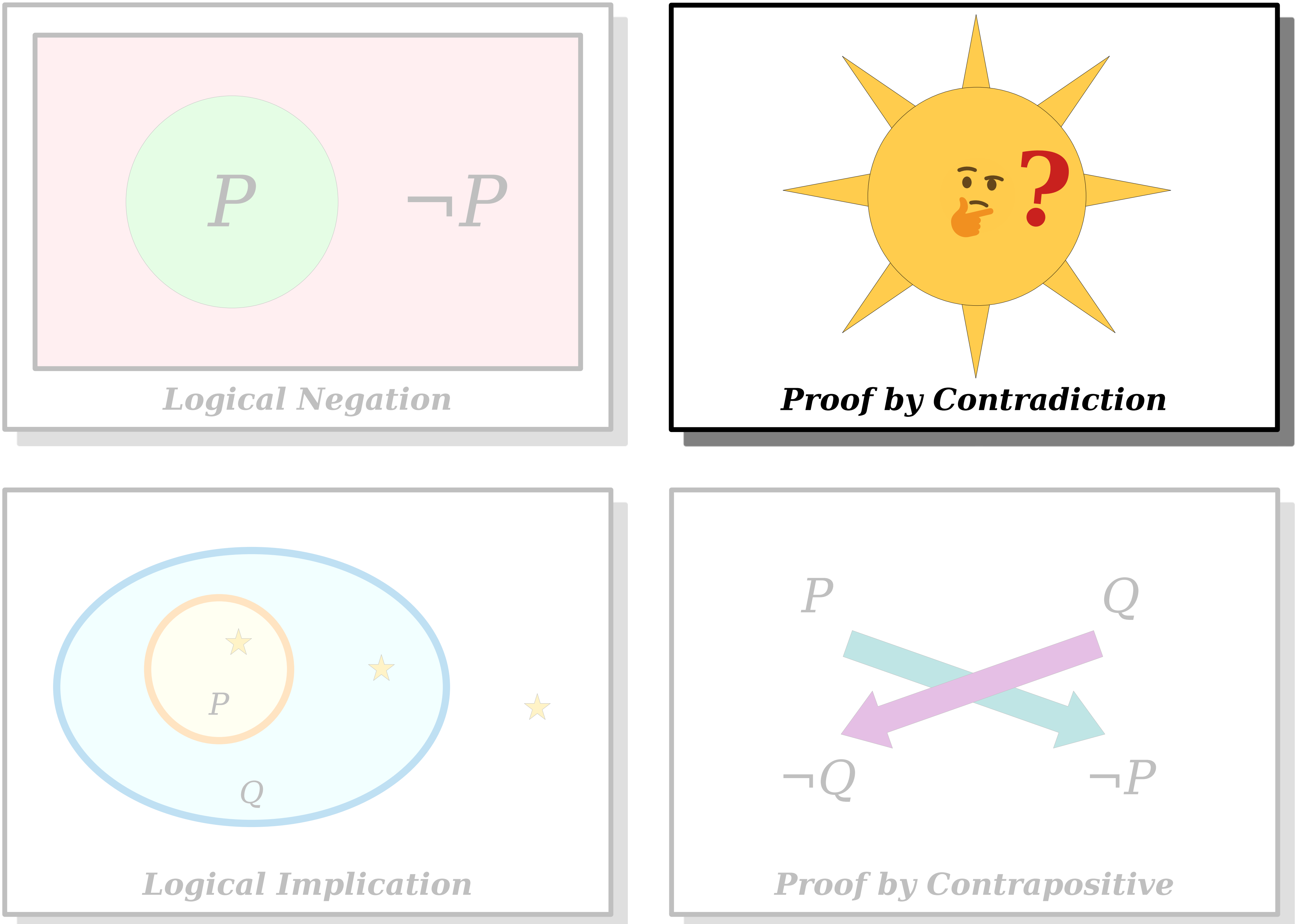
Proof by Contradiction



Logical Implication



Proof by Contrapositive


P
¬P
Logical Negation
?
Proof by Contradiction
P
Q
Logical Implication
P
Q
¬Q
¬P
Proof by Contrapositive

Act II

Proof by Contradiction

First, let’s reflect on the **direct proof** technique we saw Wednesday.

Our First Proof! (from Wednesday)

Theorem: If n is an even integer, then n^2 is even.

Our First Proof! (from Wednesday)

Theorem: If n is an even integer, then n^2 is even.

Proof: Assume n is an even integer.

Our First Proof! (from Wednesday)

Theorem: If n is an even integer, then n^2 is even.

Proof: Assume n is an even integer. We want to show that n^2 is even.

Our First Proof! (from Wednesday)

Theorem: If n is an even integer, then n^2 is even.

Proof: Assume n is an even integer. We want to show that n^2 is even.

Since n is even, there is some integer k such that $n = 2k$.

Our First Proof! (from Wednesday)

Theorem: If n is an even integer, then n^2 is even.

Proof: Assume n is an even integer. We want to show that n^2 is even.

Since n is even, there is some integer k such that $n = 2k$. This means that

$$n^2 = (2k)^2$$

Our First Proof! (from Wednesday)

Theorem: If n is an even integer, then n^2 is even.

Proof: Assume n is an even integer. We want to show that n^2 is even.

Since n is even, there is some integer k such that $n = 2k$. This means that

$$\begin{aligned} n^2 &= (2k)^2 \\ &= 4k^2 \end{aligned}$$

Our First Proof! (from Wednesday)

Theorem: If n is an even integer, then n^2 is even.

Proof: Assume n is an even integer. We want to show that n^2 is even.

Since n is even, there is some integer k such that $n = 2k$. This means that

$$
\begin{aligned}
n^2 &= (2k)^2 \\
&= 4k^2 \\
&= 2(2k^2).
\end{aligned}
$$

Our First Proof! (from Wednesday)

Theorem: If n is an even integer, then n^2 is even.

Proof: Assume n is an even integer. We want to show that n^2 is even.

Since n is even, there is some integer k such that $n = 2k$. This means that

$$\begin{aligned} n^2 &= (2k)^2 \\ &= 4k^2 \\ &= 2(2k^2). \end{aligned}$$

From this, we see that there is an integer m (namely, $2k^2$) where $n^2 = 2m$.

Our First Proof! (from Wednesday)

Theorem: If n is an even integer, then n^2 is even.

Proof: Assume n is an even integer. We want to show that n^2 is even.

Since n is even, there is some integer k such that $n = 2k$. This means that

$$\begin{aligned} n^2 &= (2k)^2 \\ &= 4k^2 \\ &= 2(2k^2). \end{aligned}$$

From this, we see that there is an integer m (namely, $2k^2$) where $n^2 = 2m$. Therefore, n^2 is even, which is what we wanted to show.

Our First Proof! (from Wednesday)

Theorem: If n is an even integer, then n^2 is even.

Proof: Assume n is an even integer. We want to show that n^2 is even.

Since n is even, there is some integer k such that $n = 2k$. This means that

$$\begin{aligned} n^2 &= (2k)^2 \\ &= 4k^2 \\ &= 2(2k^2). \end{aligned}$$

From this, we see that there is an integer m (namely, $2k^2$) where $n^2 = 2m$. Therefore, n^2 is even, which is what we wanted to show. ■

Our First Proof! (from Wednesday)

Theorem: If n is an even integer, then n^2 is even.

Proof: Assume n is an even integer. We want to show that n^2 is even.

Since n is even, there is some integer k such that $n = 2k$. This means that

n

From this, we se
(namely, $2k^2$) wh
is even, which is

To prove

"If *P* is true, then *Q* is true,"

we start by asking our reader to assume ***P*** is true.

Our First Proof! (from Wednesday)

Theorem: If n is an even integer, then n^2 is even.

Proof: Assume n is an even integer. We want to show that n^2 is even.

Since n is even, there is some integer k such that $n = 2k$. This means that

$$n^2 = (2k)^2$$

If we apply **sound logic** (using definitions, algebra, etc.) all the statements that follow are **also true.**

From this,
(namely, $2k^2$) where $n^2 = 2m$. Therefore, n^2 is even, which is what we wanted to show. ■

Our First Proof! (from Wednesday)

Theorem: If n is an even integer, then n^2 is even.

> If we apply **sound logic** (using definitions, algebra, etc.) all the statements that follow are **also true.**

Proof: Assum
show that n

Since n is ev
that $n = 2k$. This means that

$$n^2 = (2k)^2 = 4k^2 = 2(2k^2).$$

From this, we see that there is an integer m (namely, $2k^2$) where $n^2 = 2m$. Therefore, n^2 is even, which is what we wanted to show. ■

Our First Proof! (from Wednesday)

Theorem: If n is an even integer, then n^2 is even.

Proof: Assume n is an even integer. We want to show that n^2 is even.

Since n is even, there is some integer k such

> If we apply **sound logic** (using definitions, algebra, etc.) all the statements that follow are **also true.**

From this, we see that there is an integer m (namely, $2k^2$) where $n^2 = 2m$. Therefore, n^2 is even, which is what we wanted to show. ■

More generally speaking,

the process looks like this:

Direct Proof

We start with a statement (or statements) we know (or assume) to be true.

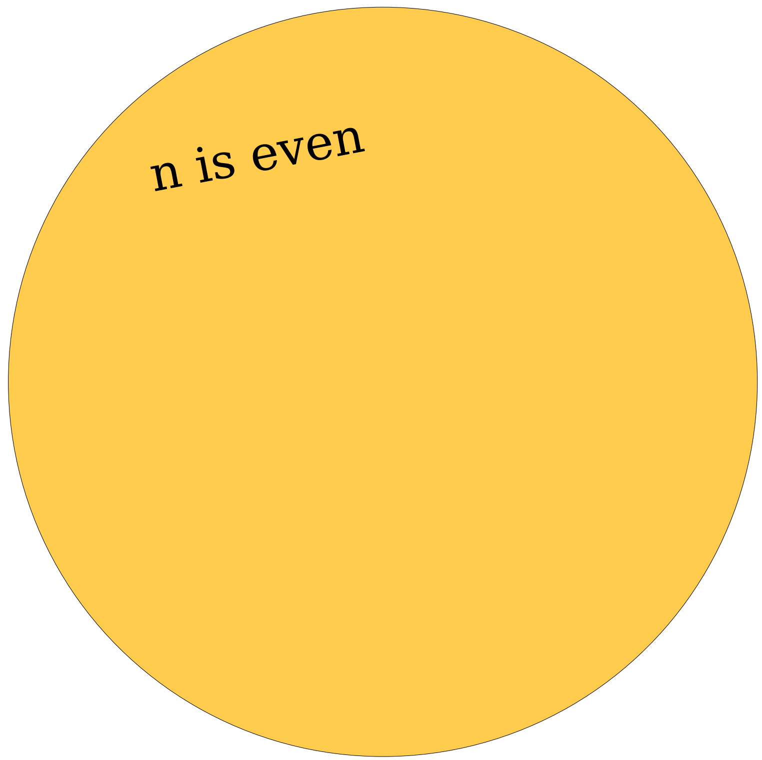
Direct Proof

We start with a statement (or statements) we know (or assume) to be true.

n is even

Direct Proof

We start with a statement (or statements) we know (or assume) to be true.



Direct Proof

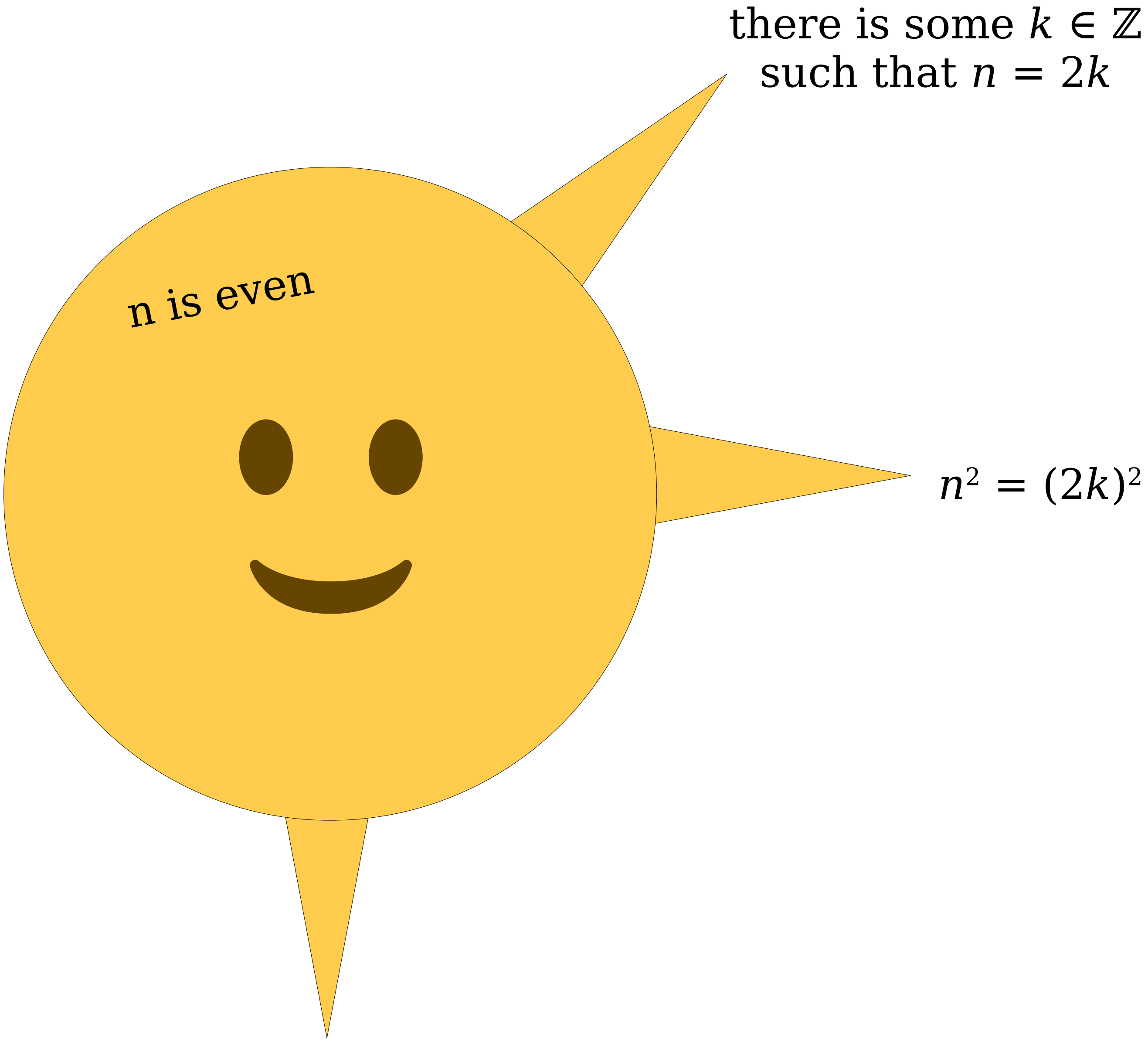
We start with a statement (or statements) we know (or assume) to be true.

Direct Proof

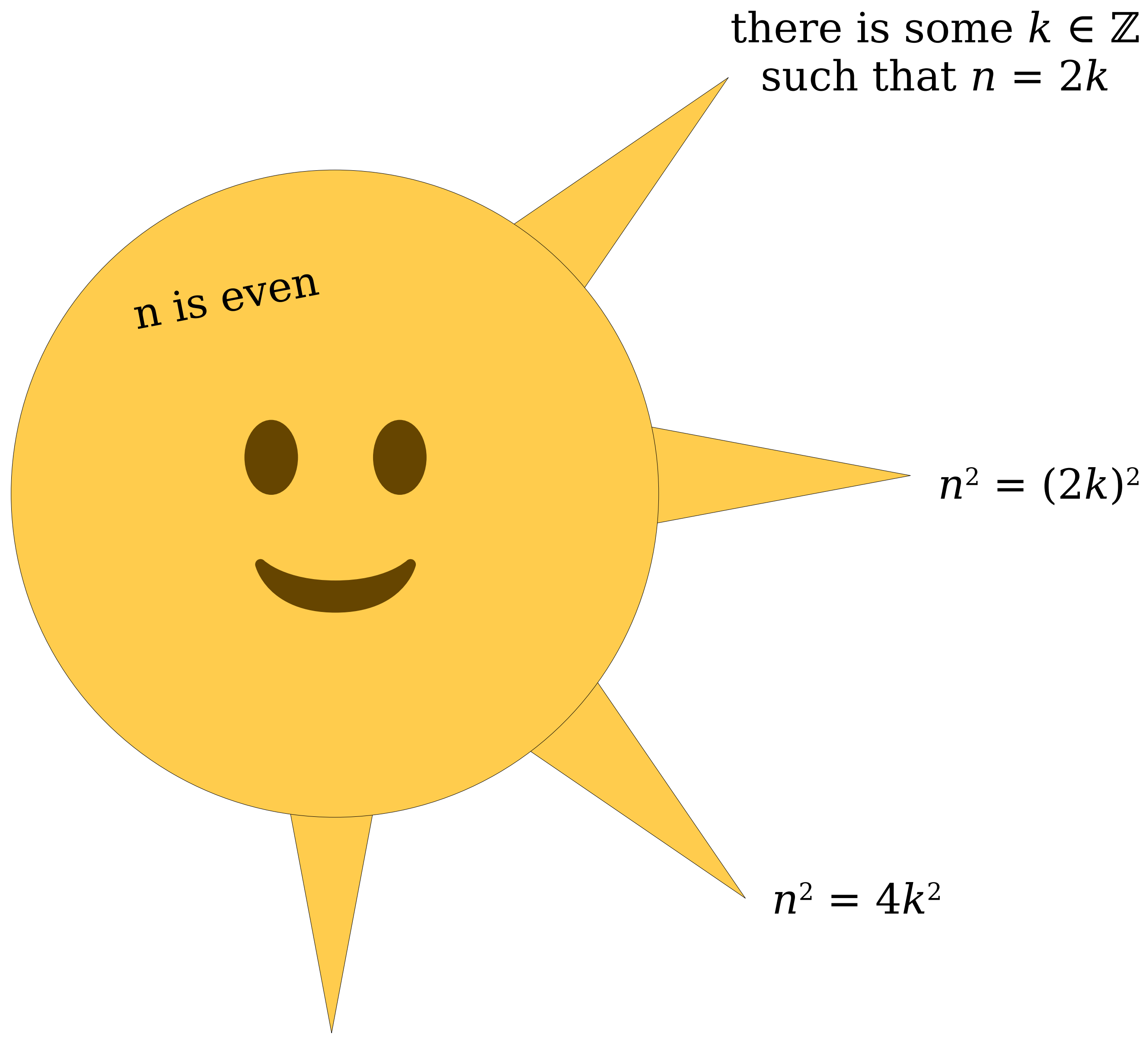
Next, we apply sound logic and rational argument to arrive at other true statements!

Direct Proof

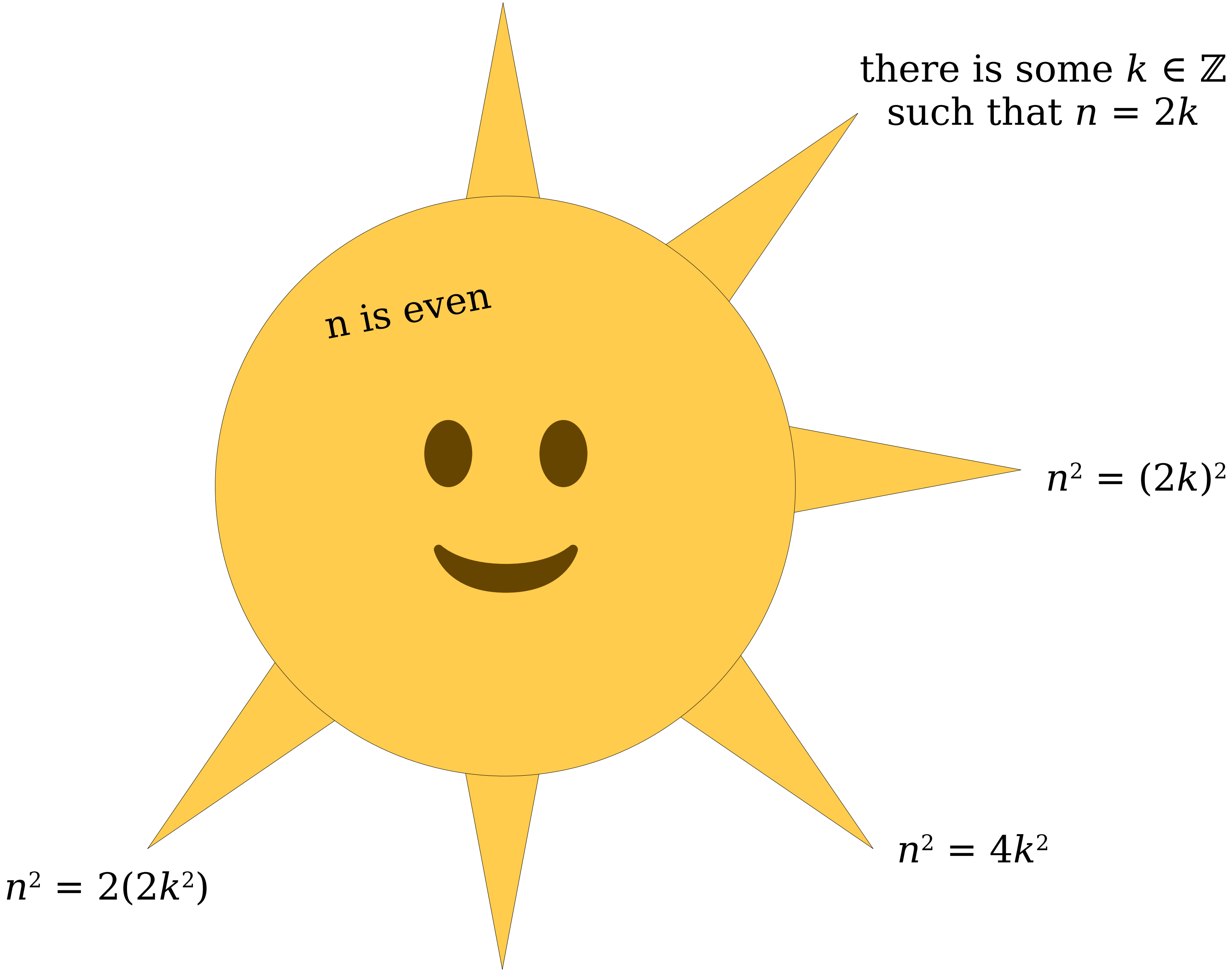
Direct Proof



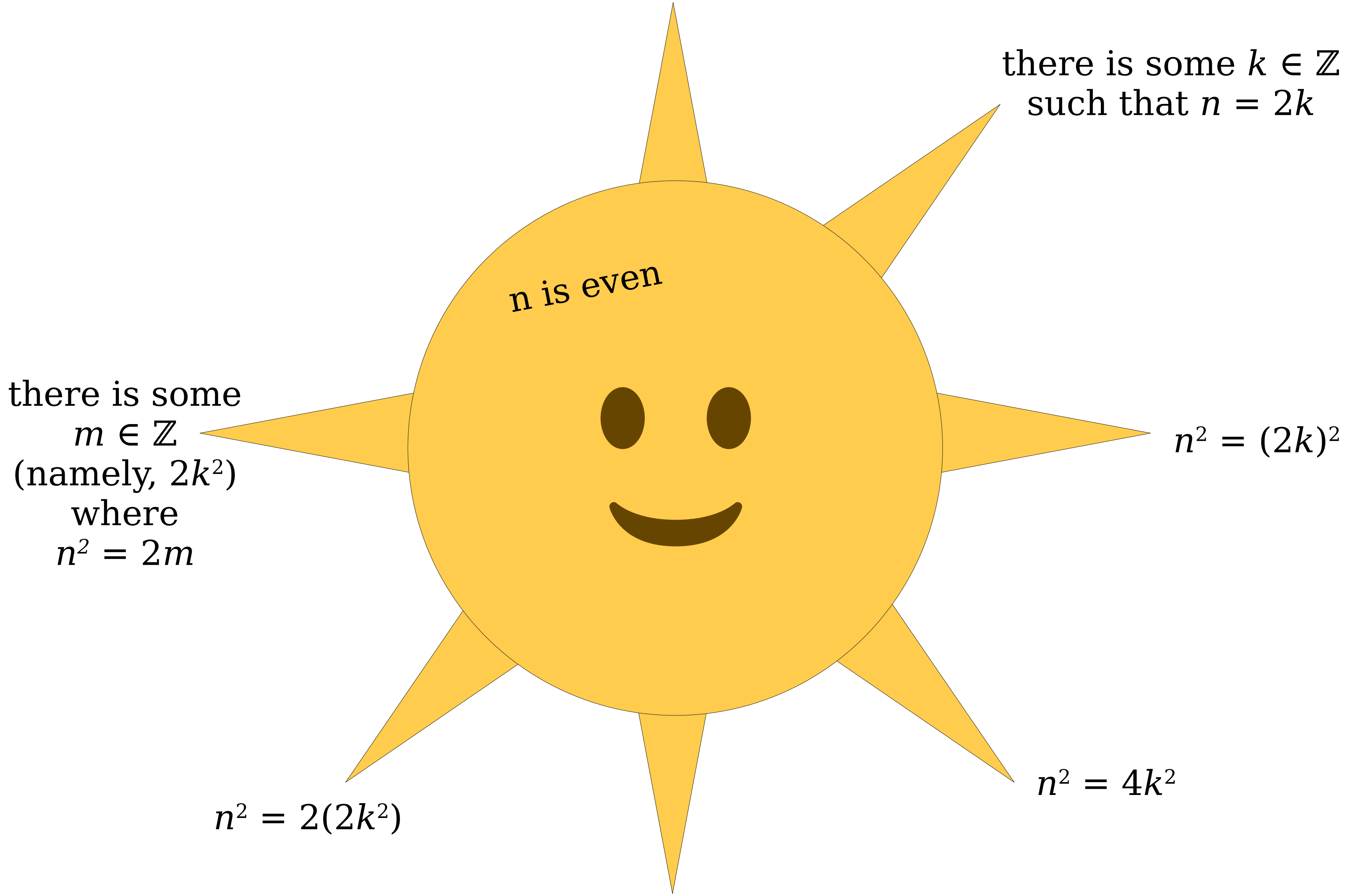
Direct Proof



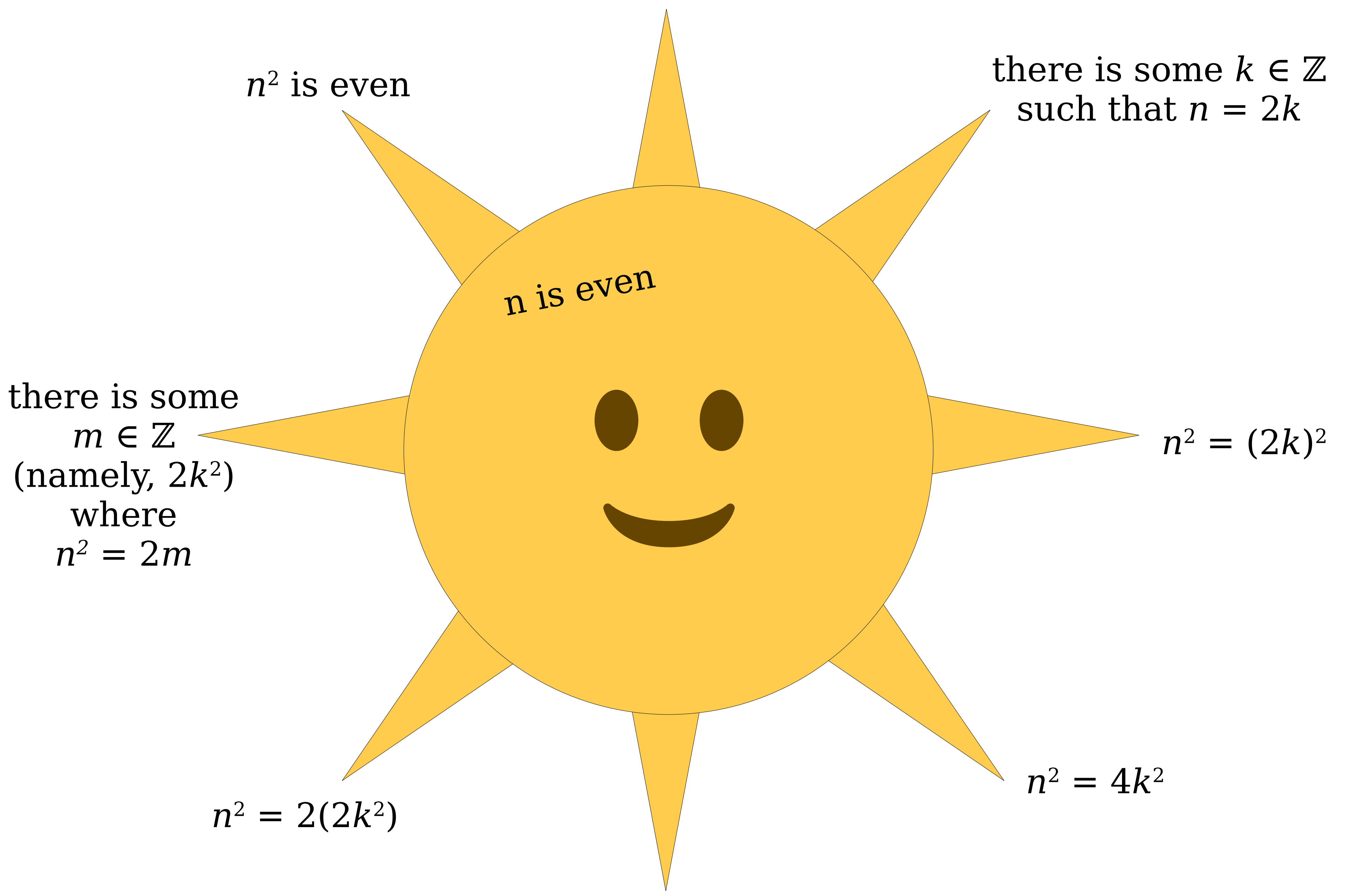
Direct Proof



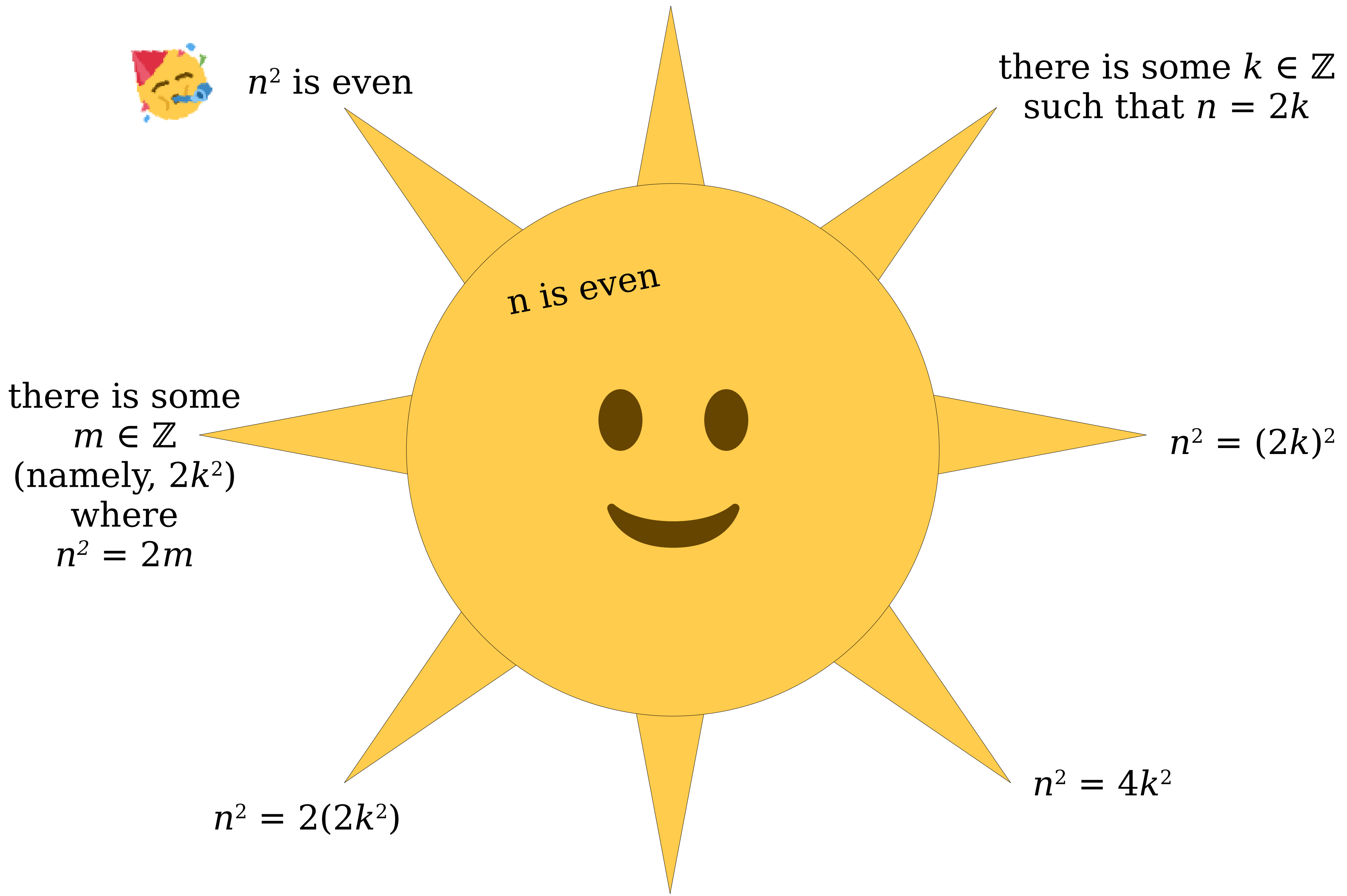
Direct Proof



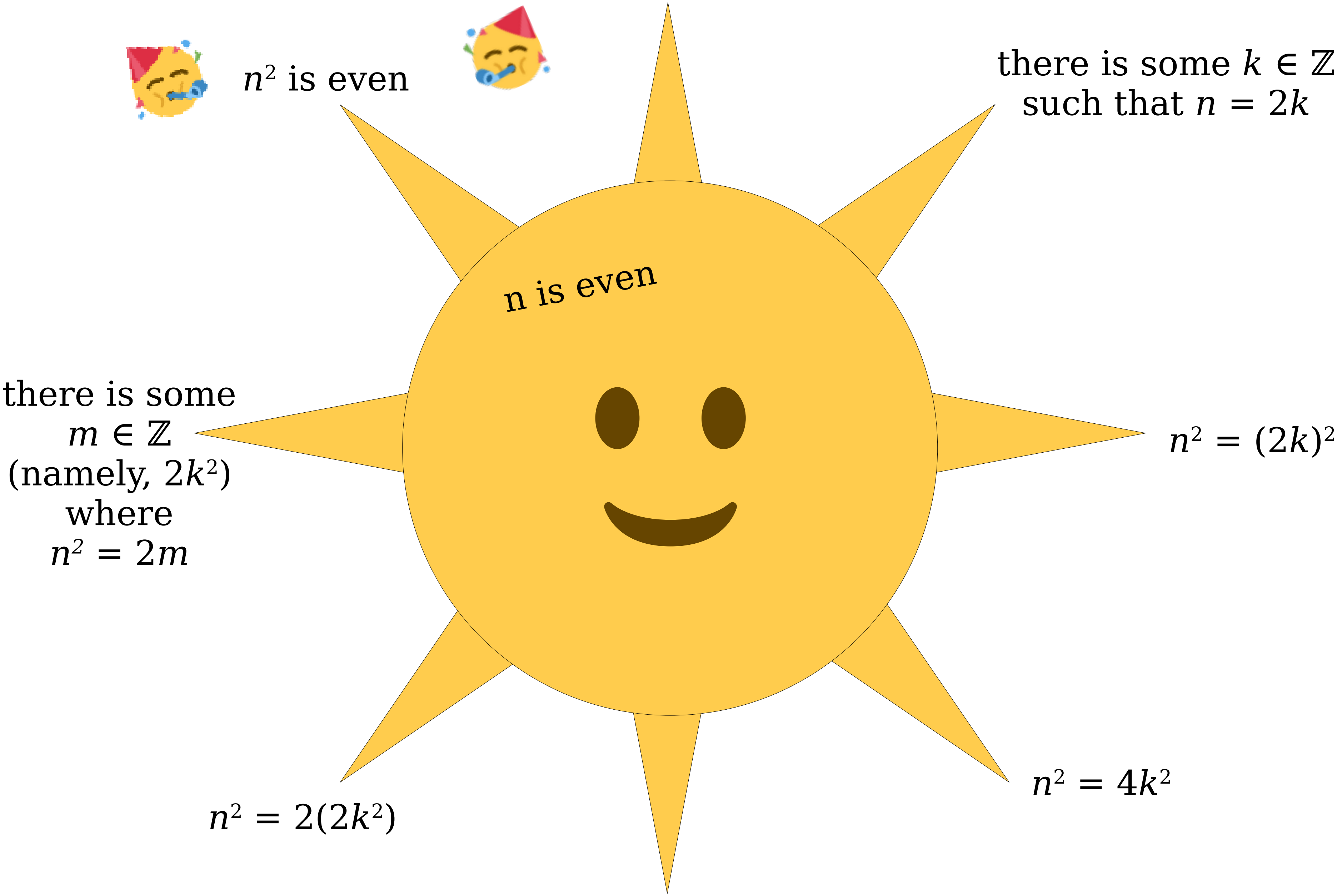
Direct Proof



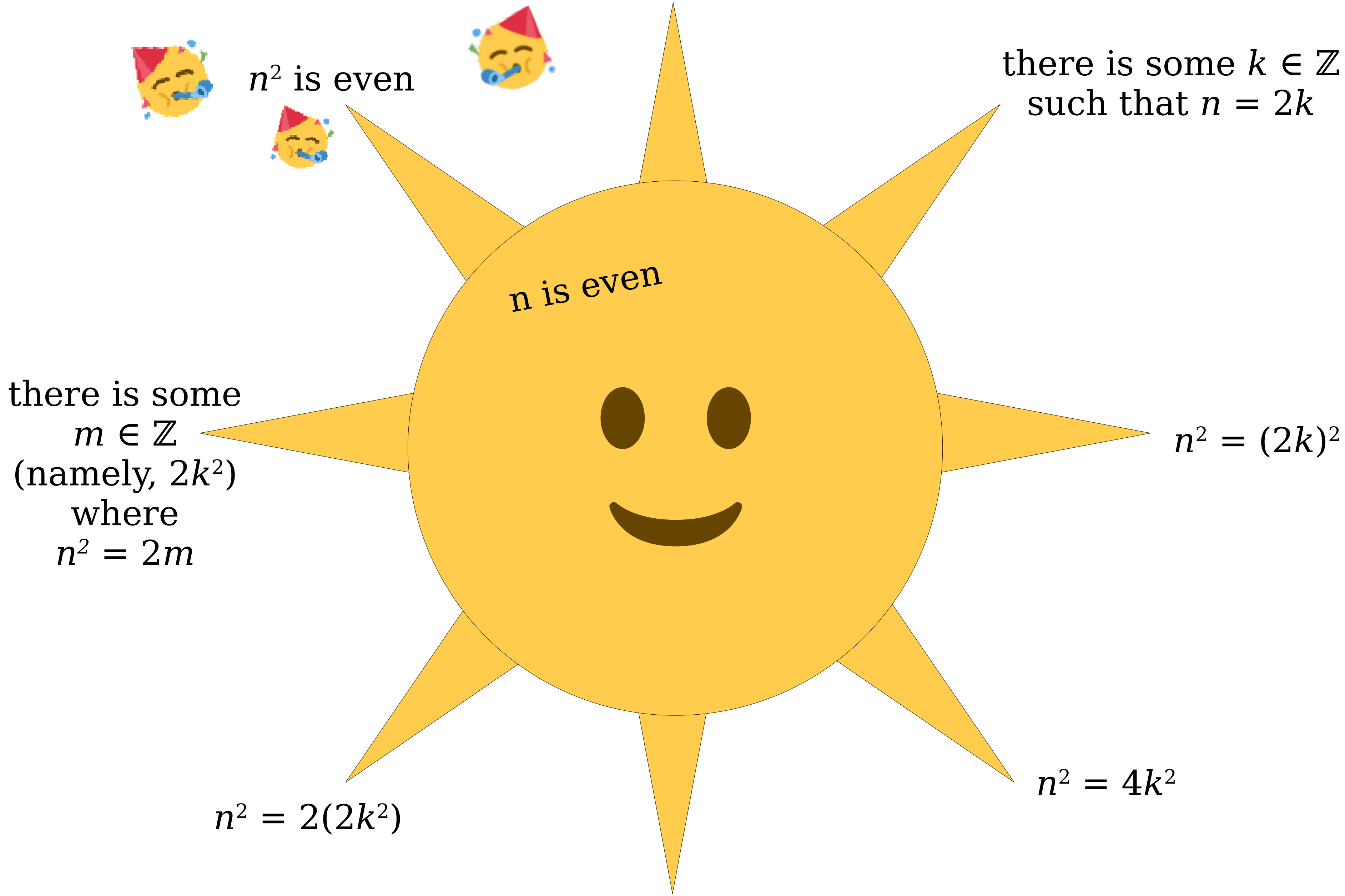
Direct Proof



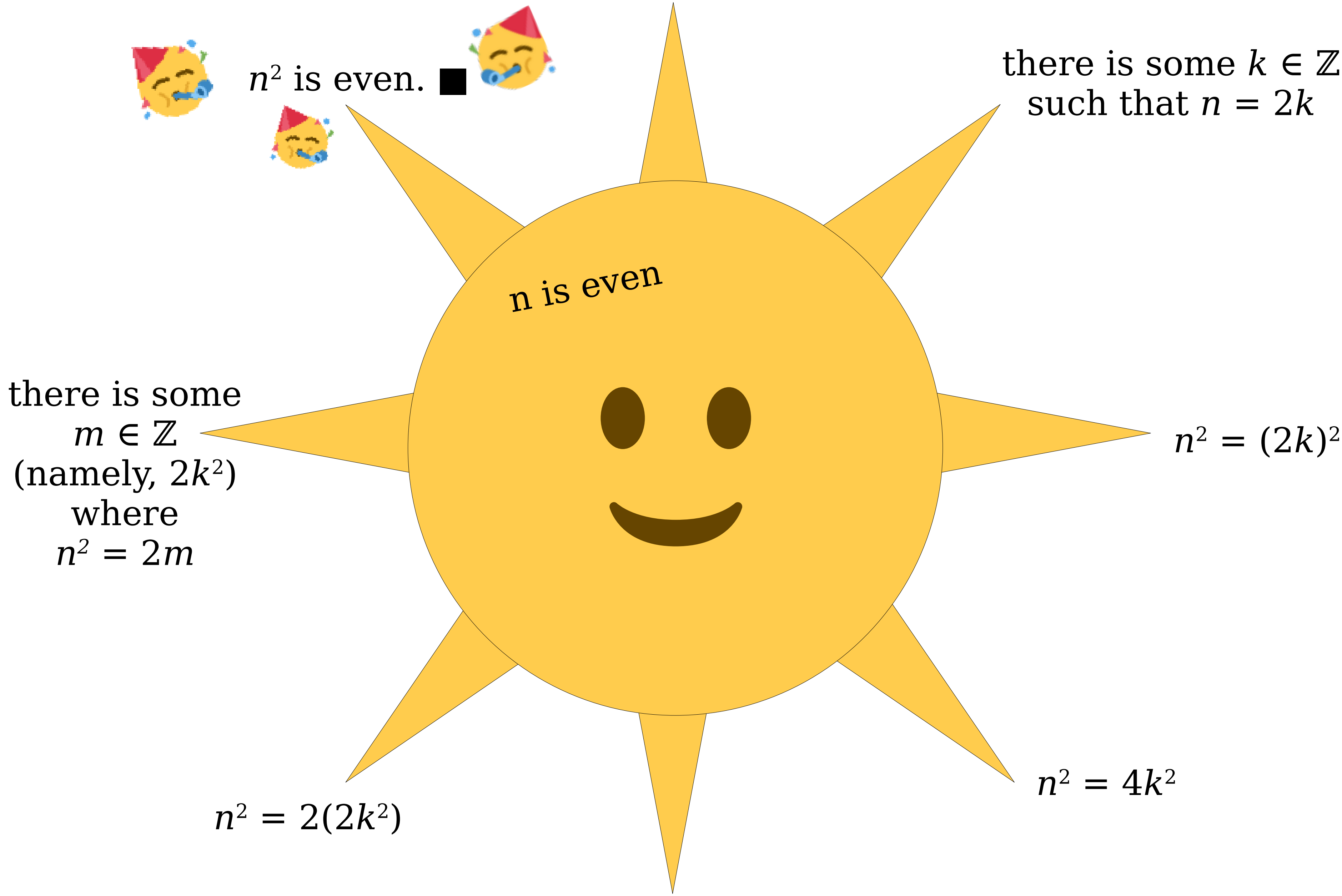
Direct Proof



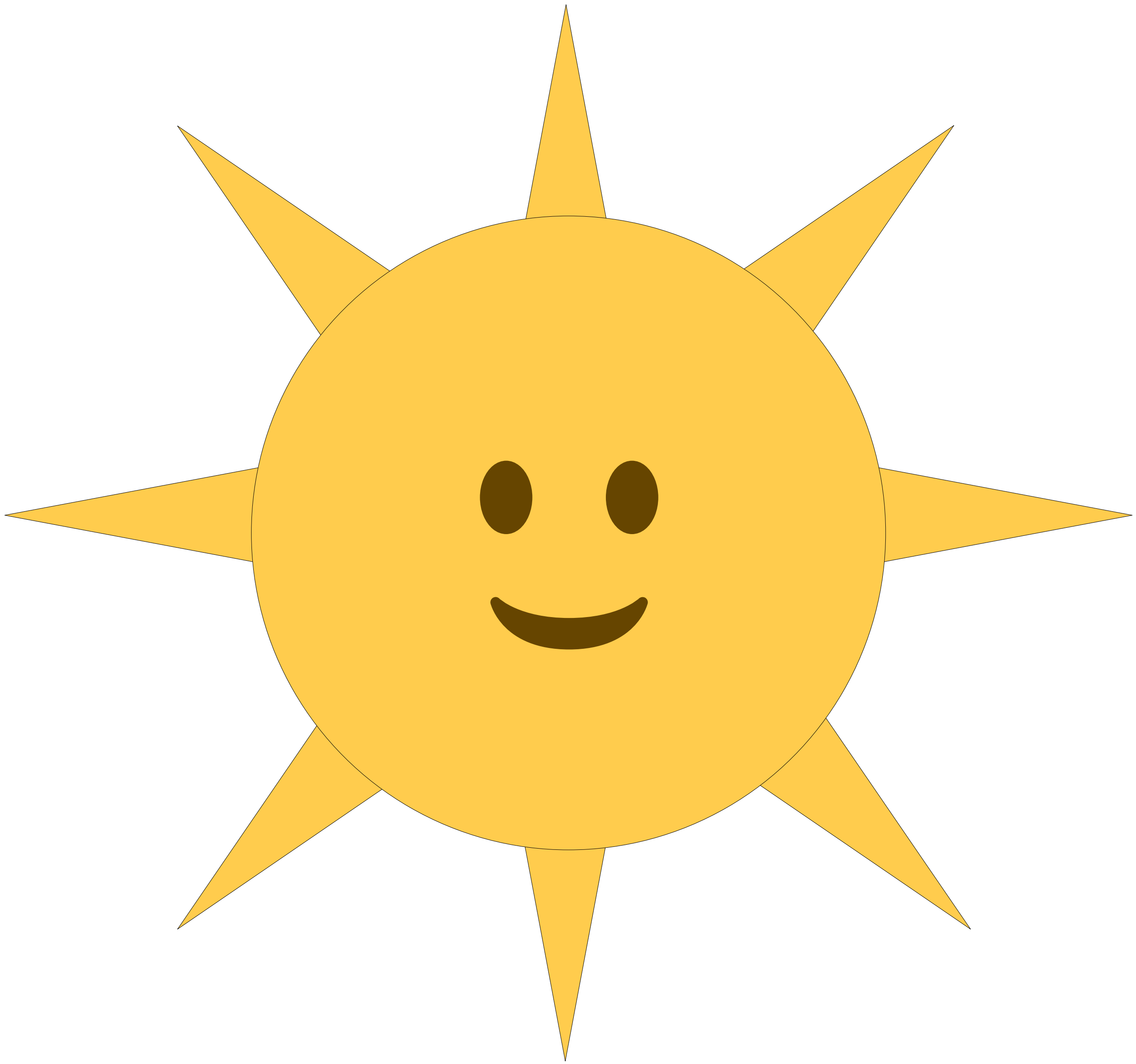
Direct Proof



Direct Proof

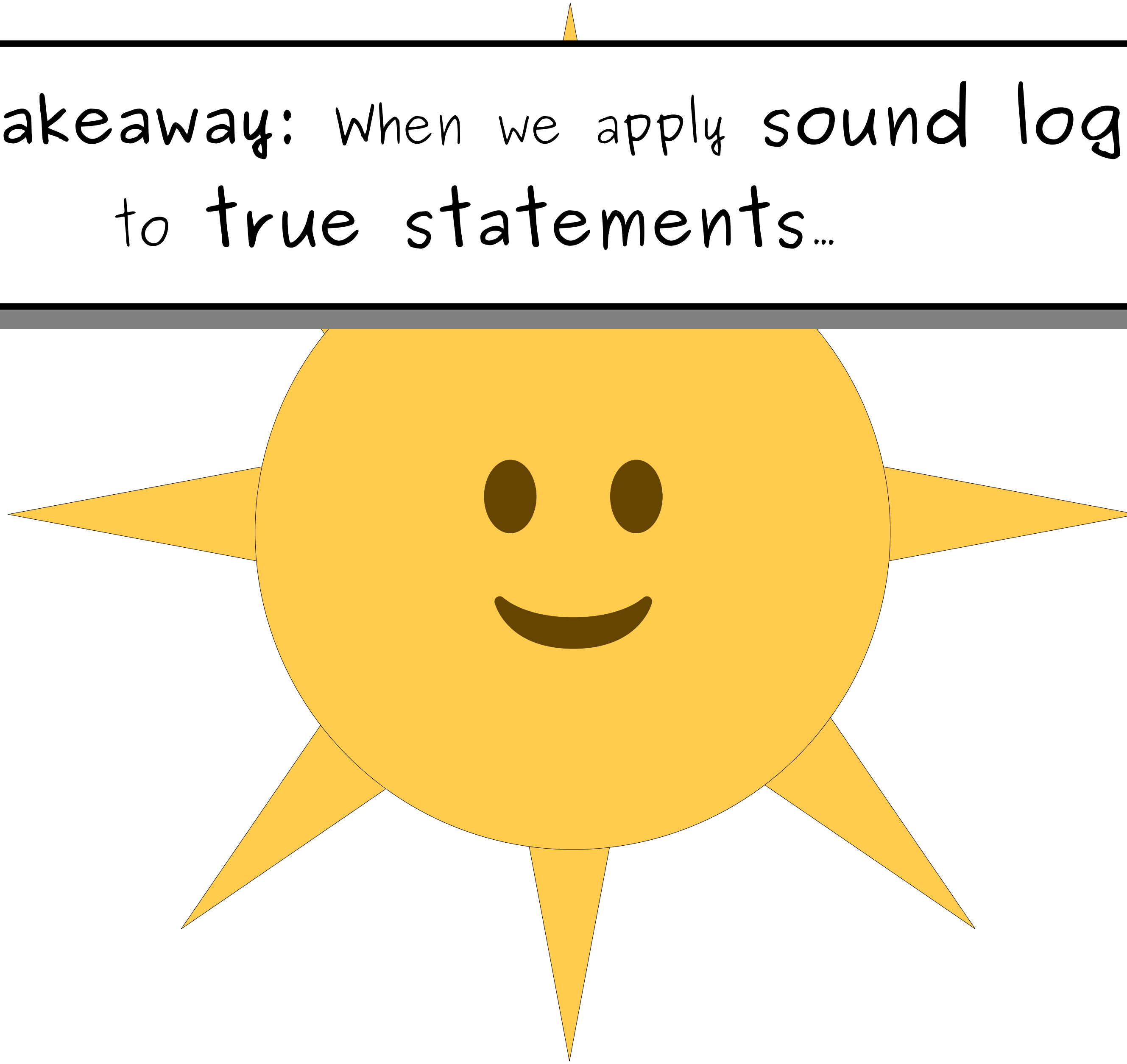


Direct Proof



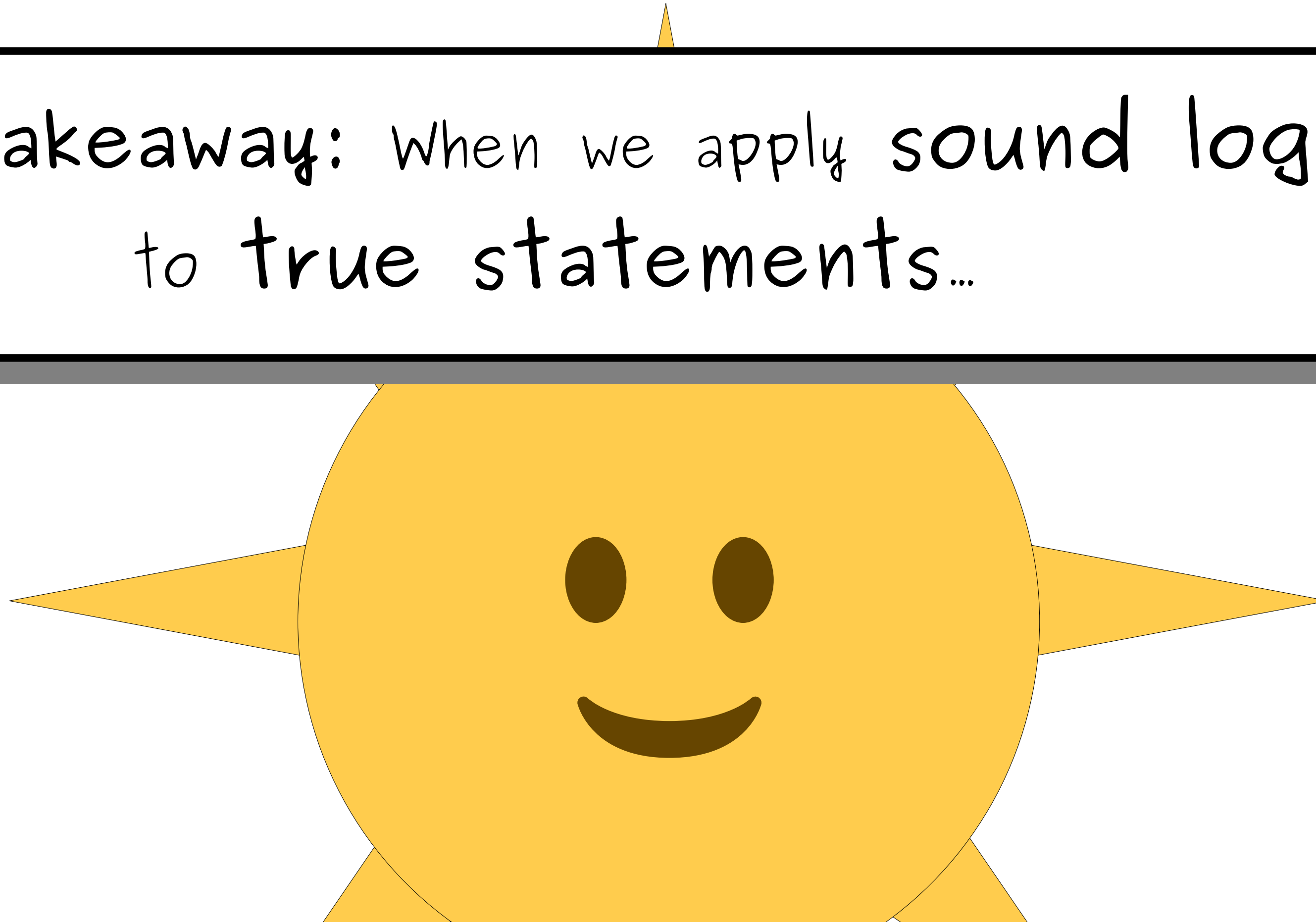
Direct Proof

Key Takeaway: When we apply **sound logic** to **true statements**…



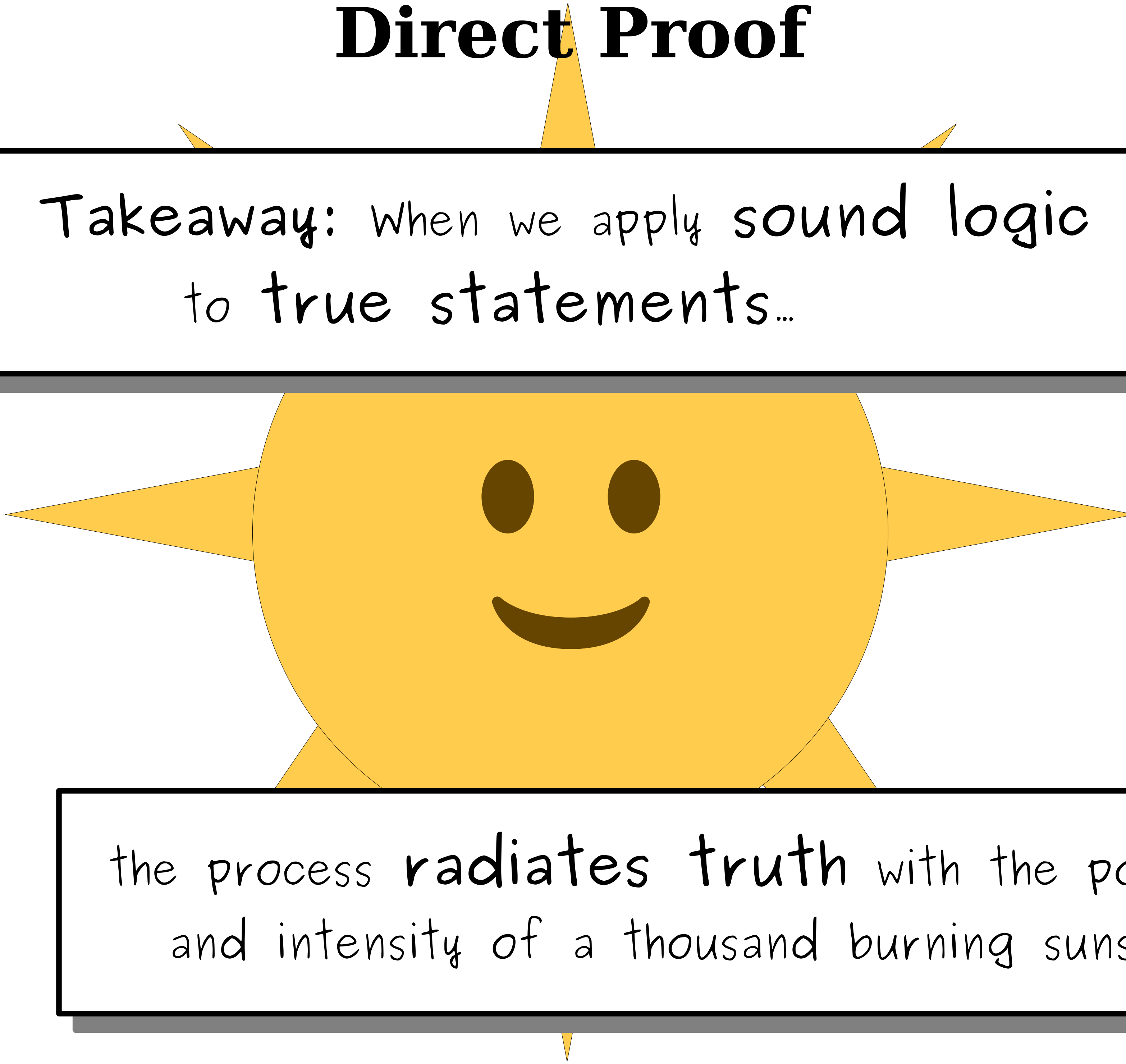
Direct Proof

Key Takeaway: When we apply **sound logic** to **true statements**…



the process **radiates truth** with the power and intensity of a thousand burning suns!

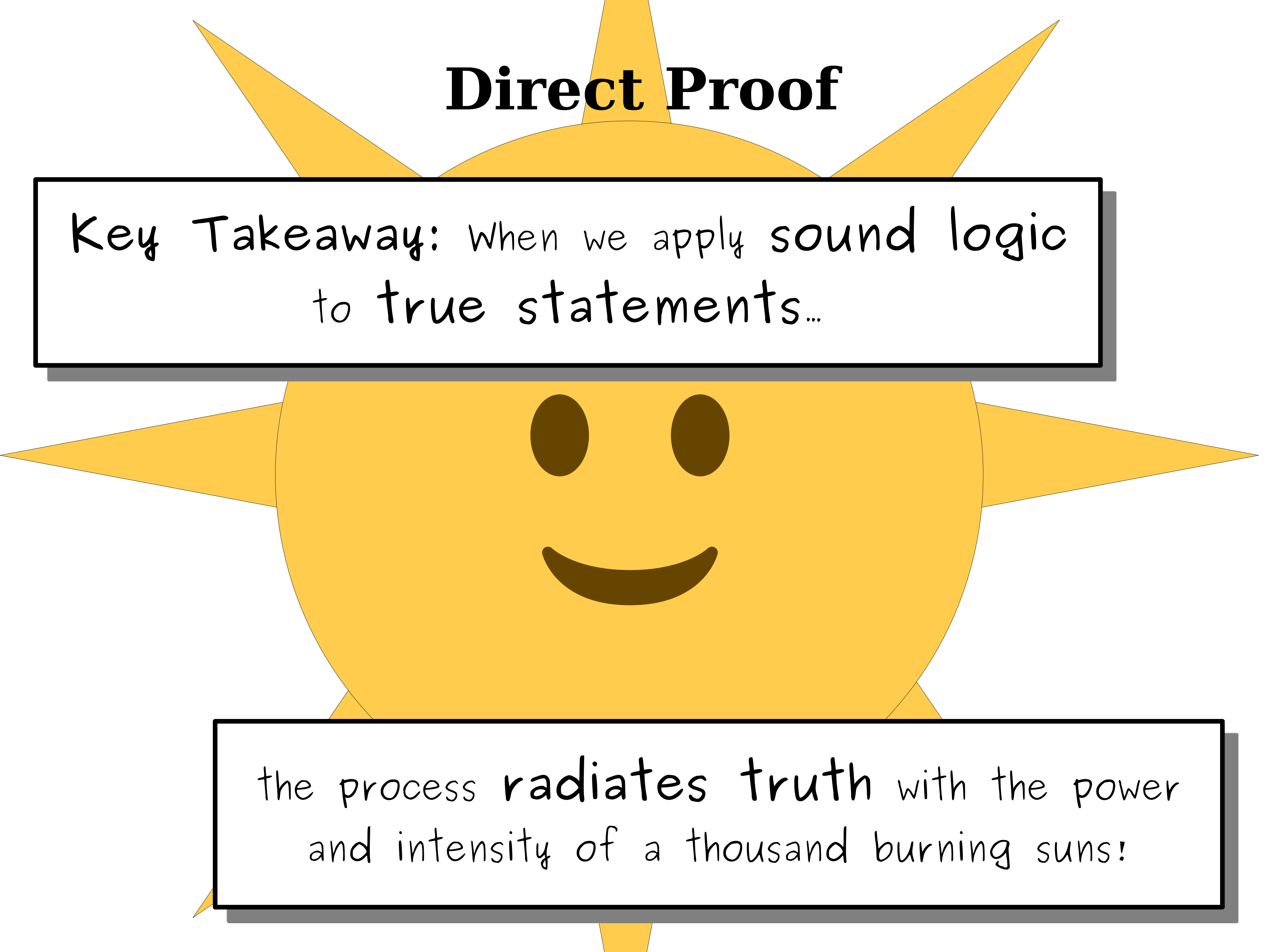
Direct Proof



Key Takeaway: When we apply **sound logic** to **true statements**…

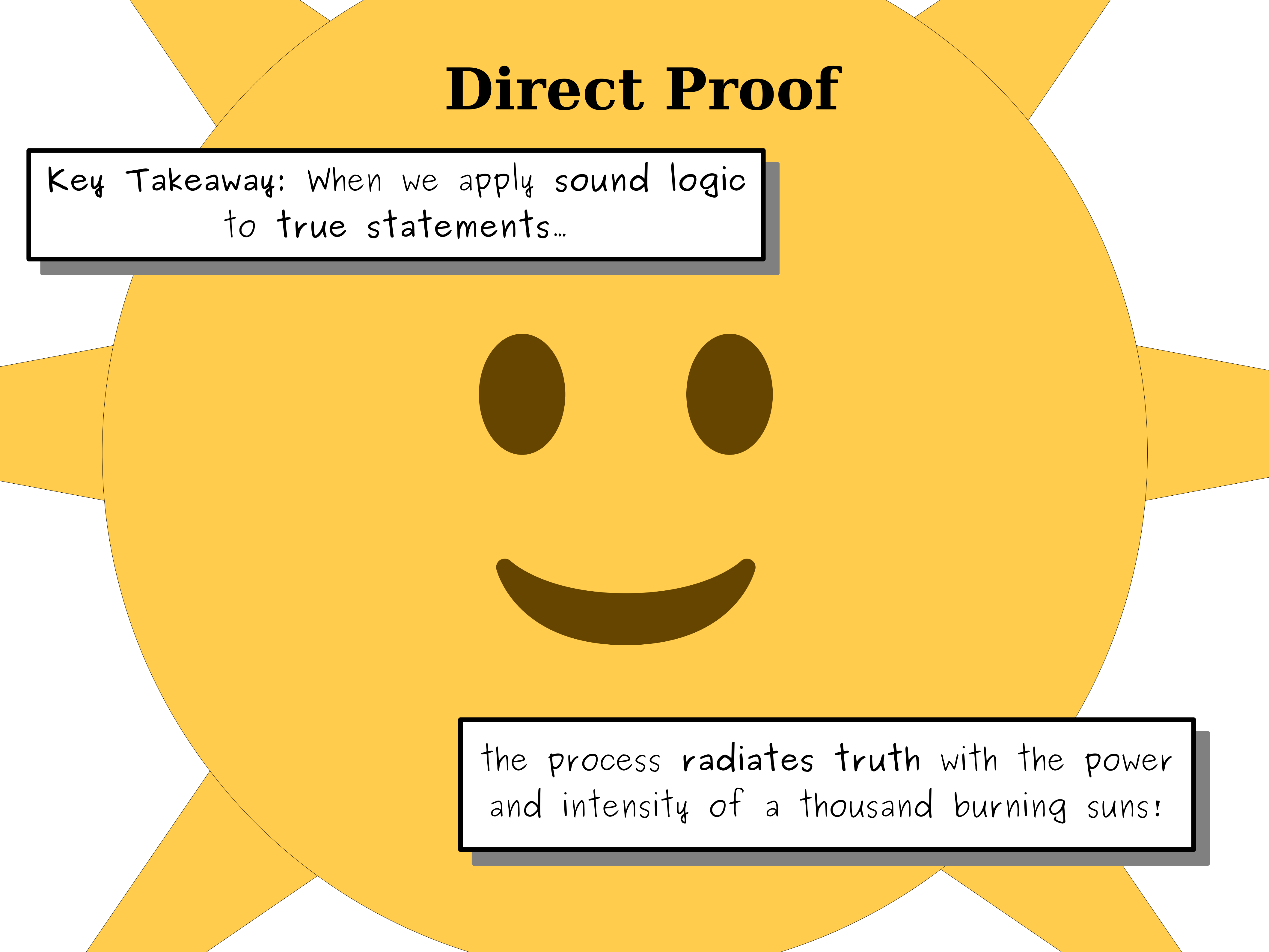
the process **radiates truth** with the power and intensity of a thousand burning suns!

Direct Proof



Key Takeaway: When we apply **sound logic** to **true statements**…

the process **radiates truth** with the power and intensity of a thousand burning suns!

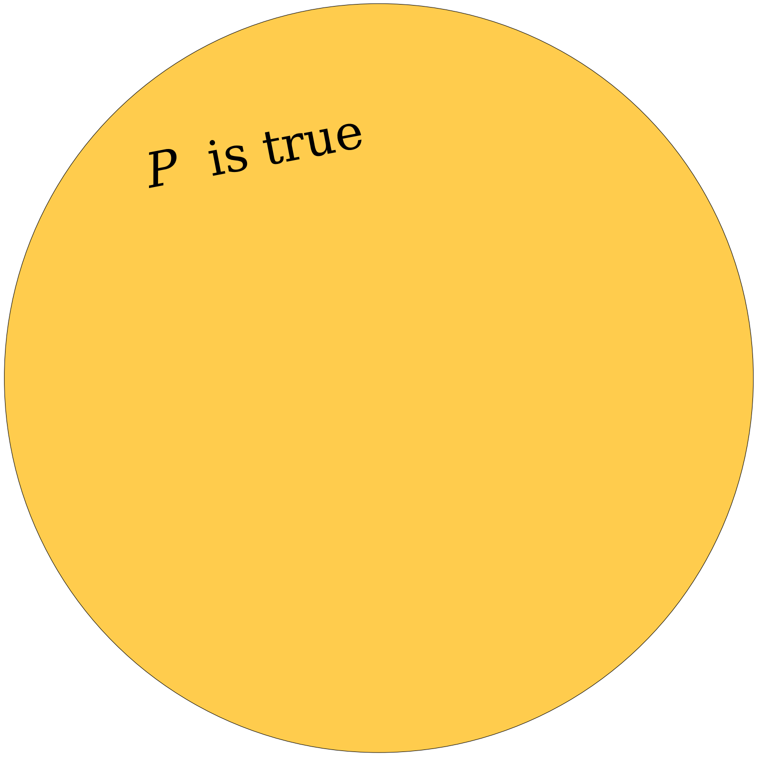

Direct Proof
Key Takeaway: When we apply sound logic to true statements…
the process radiates truth with the power and intensity of a thousand burning suns!

Okay, but…

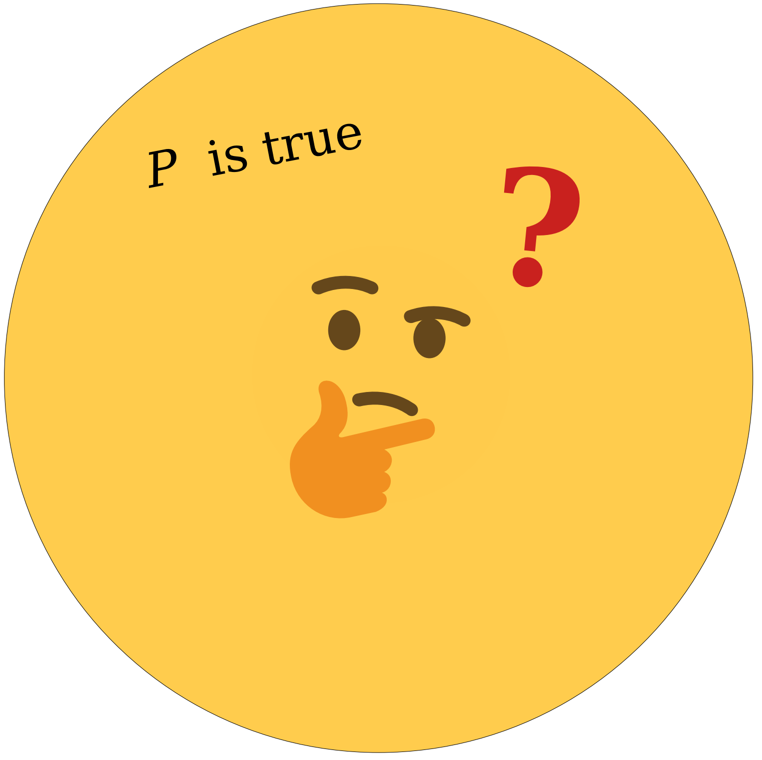
Okay, but…

what if we start with a proposition

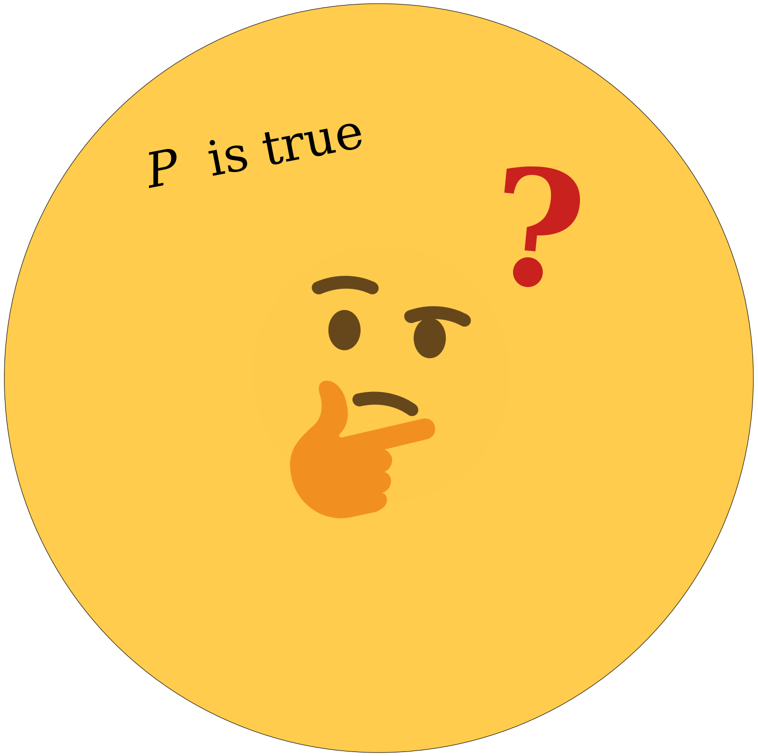
whose **truthiness** is **unknown** to us?


P is true

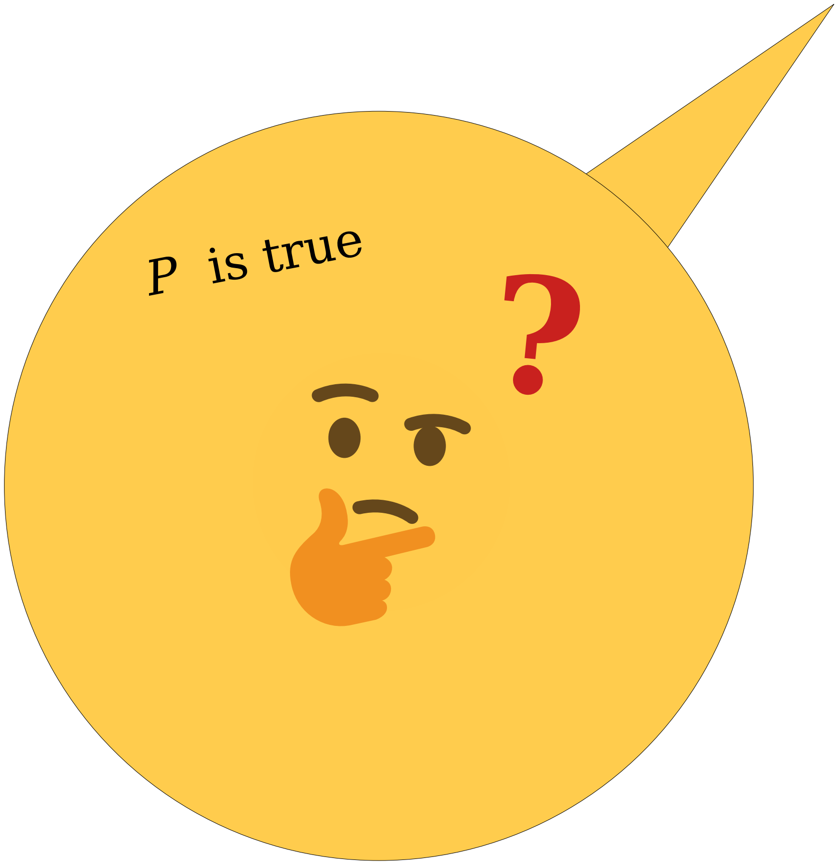

P is true


P is true
?

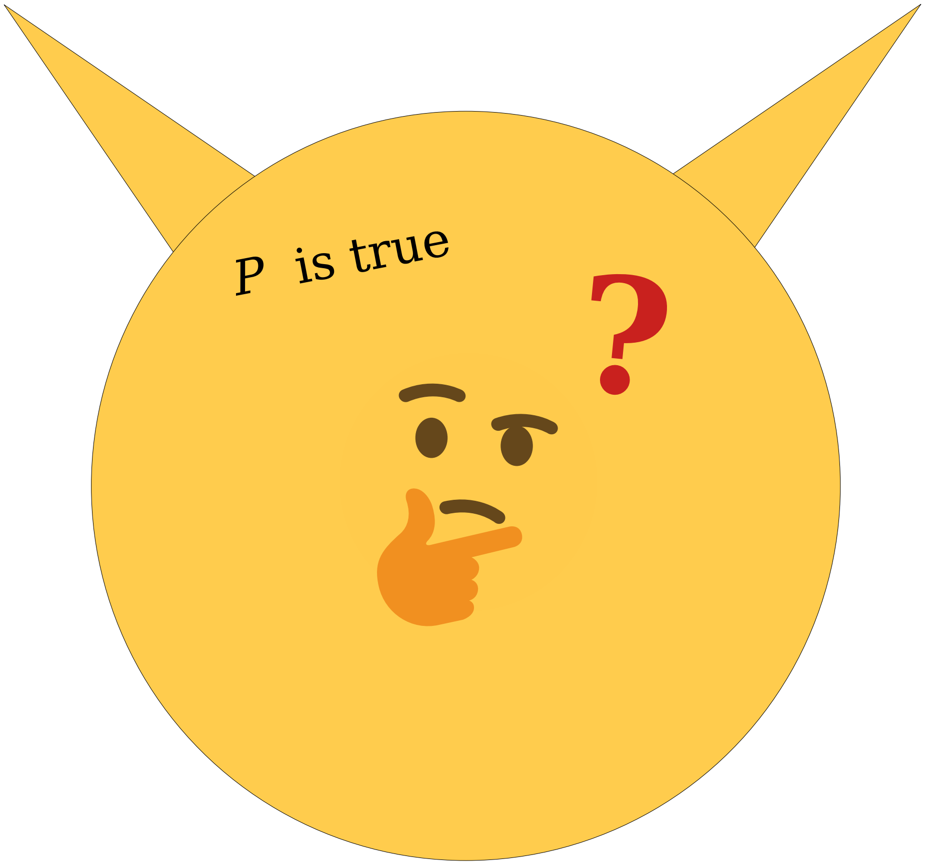
This might radiate SOME truth.



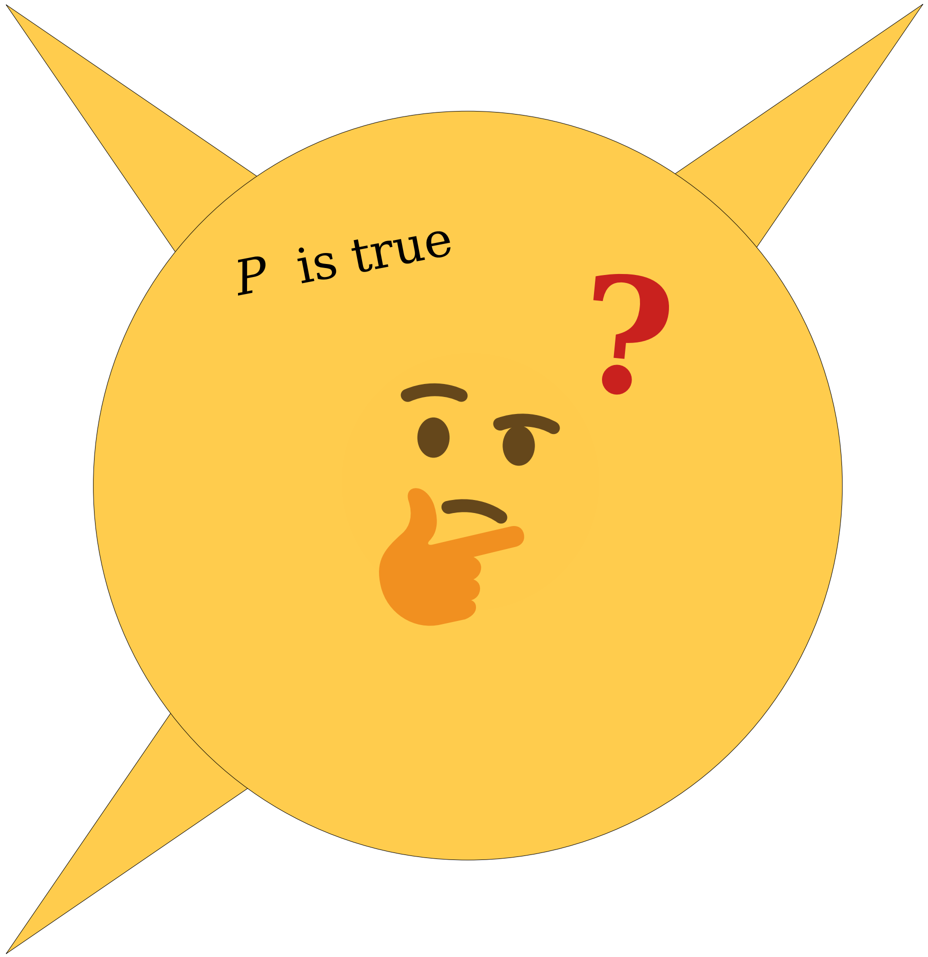
This might radiate SOME truth.



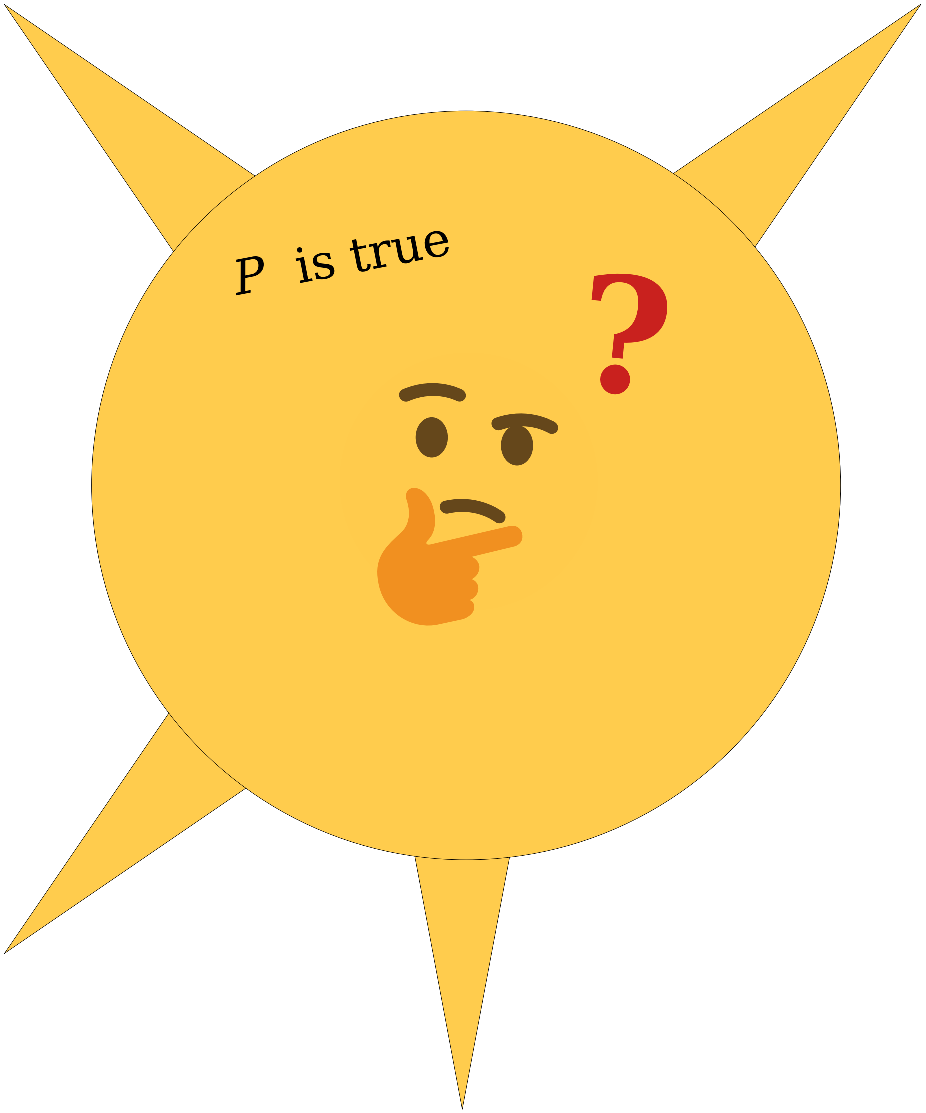
This might radiate SOME truth.



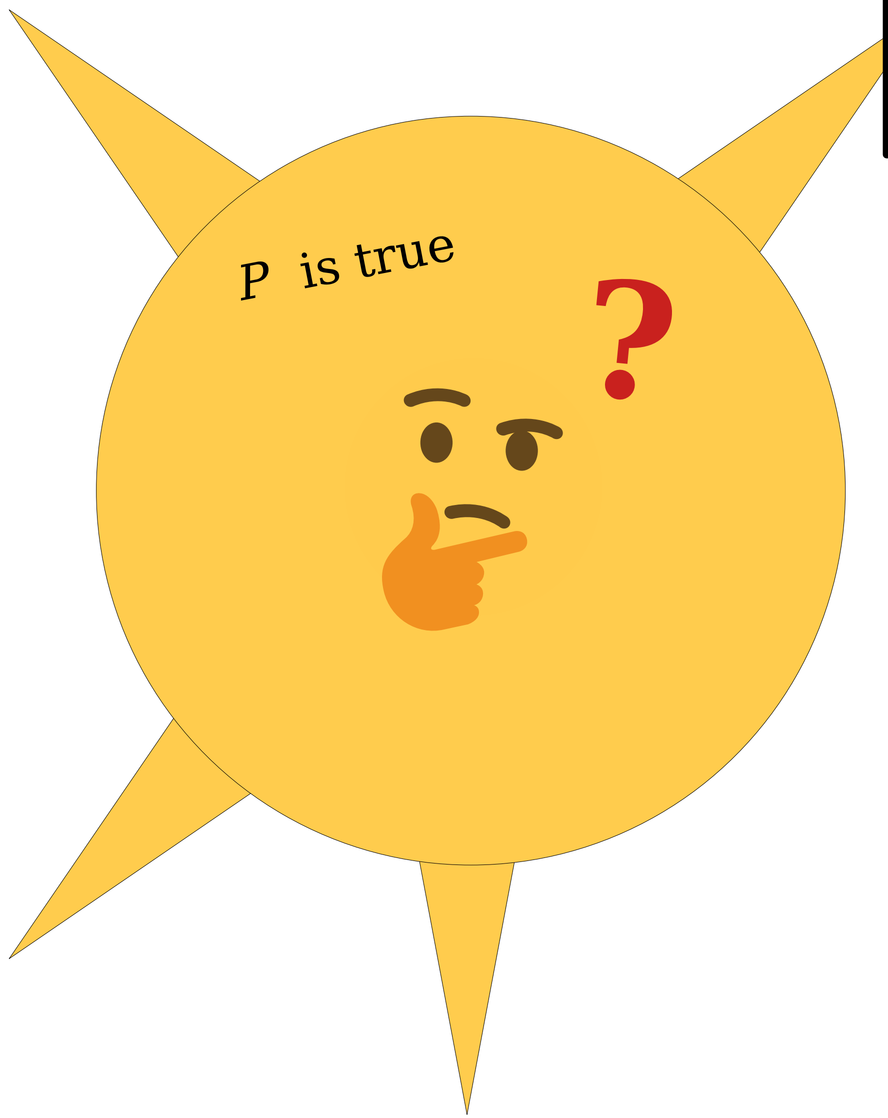
This might radiate SOME truth.



This might radiate SOME truth.



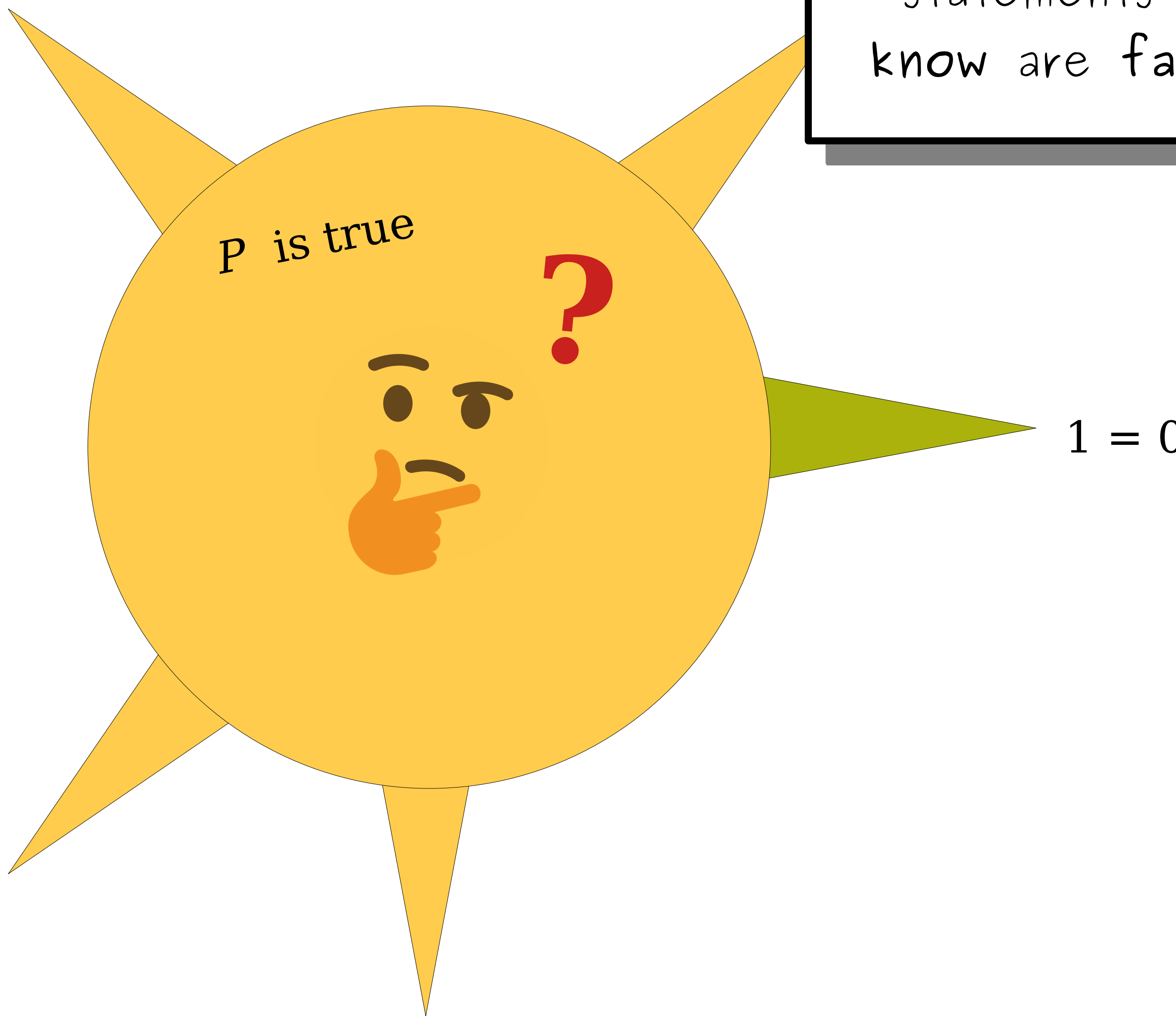
This might **radiate** **SOME truth.**



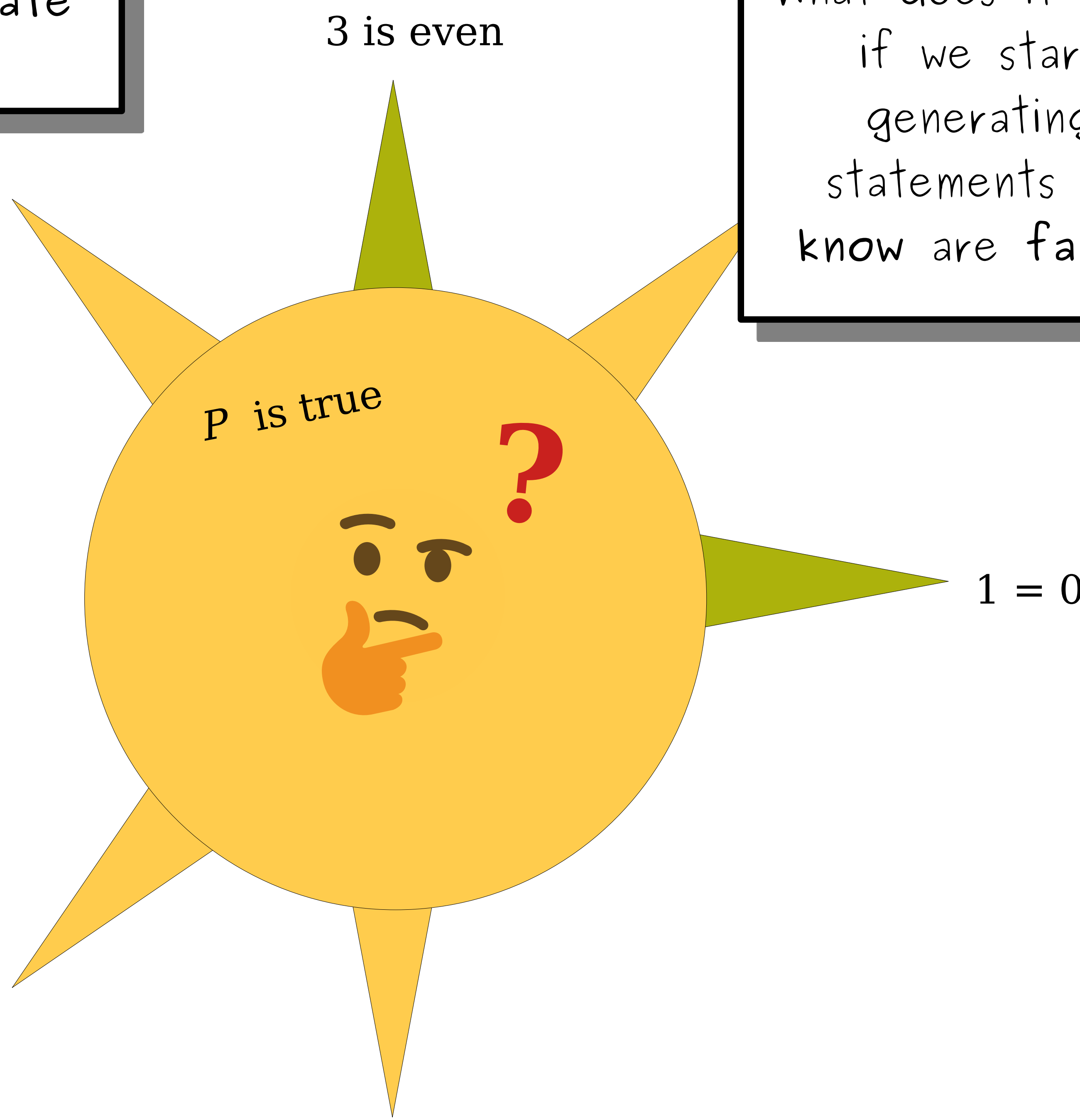
What **does** it mean if we start generating statements we **know** are **false**?

This might radiate **SOME truth.**

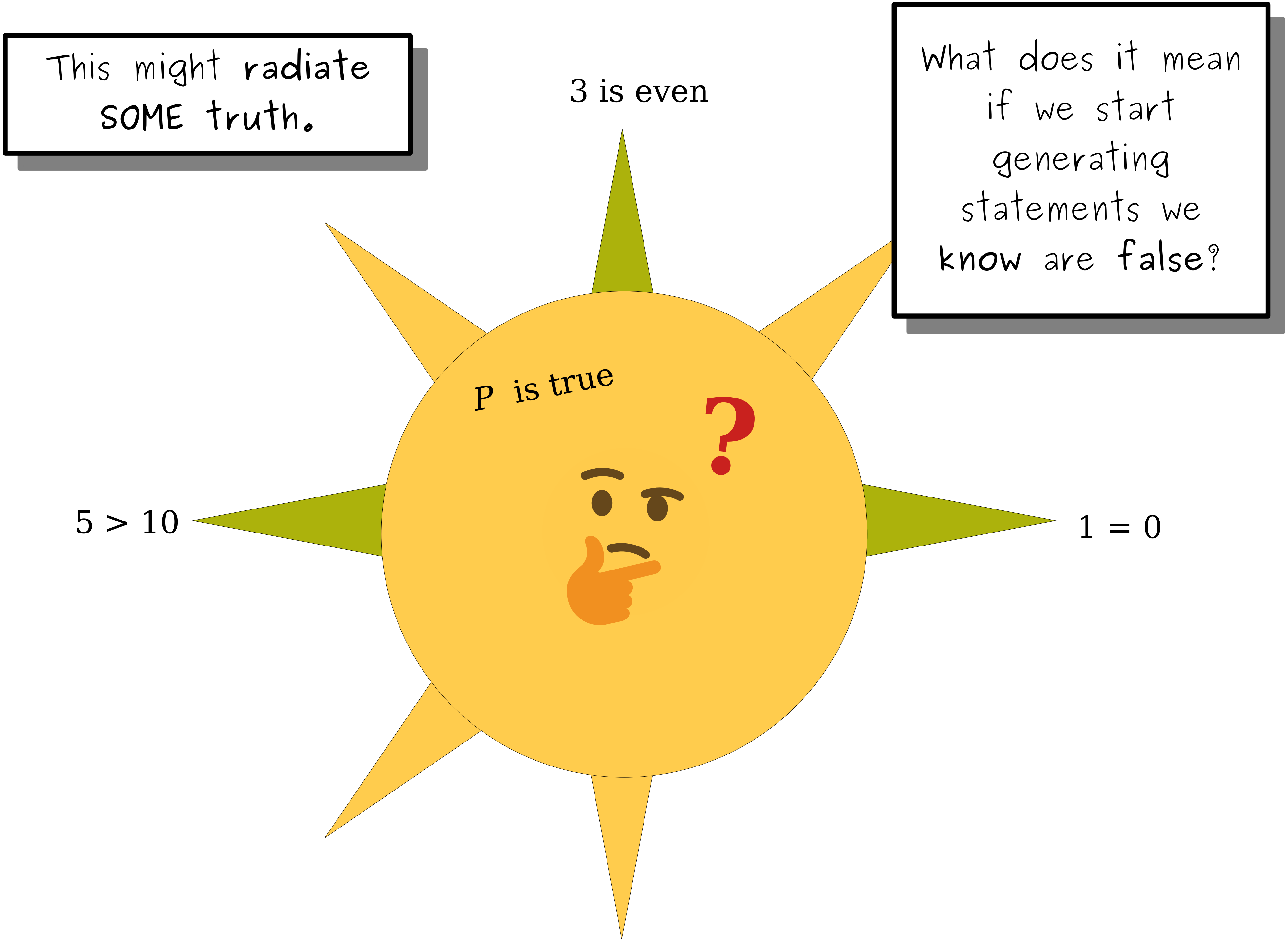
What does it mean if we start generating statements we **know** are **false**?

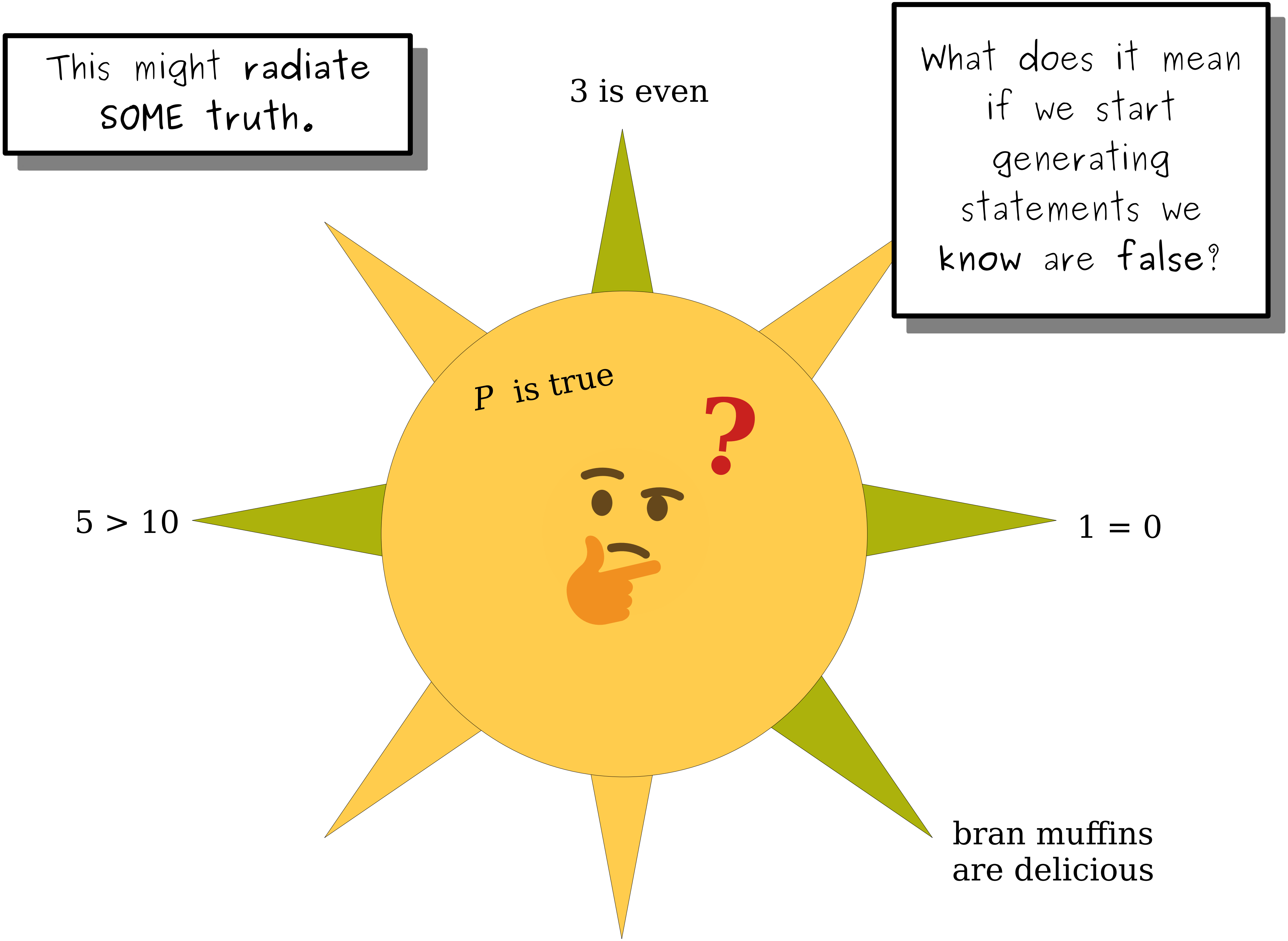


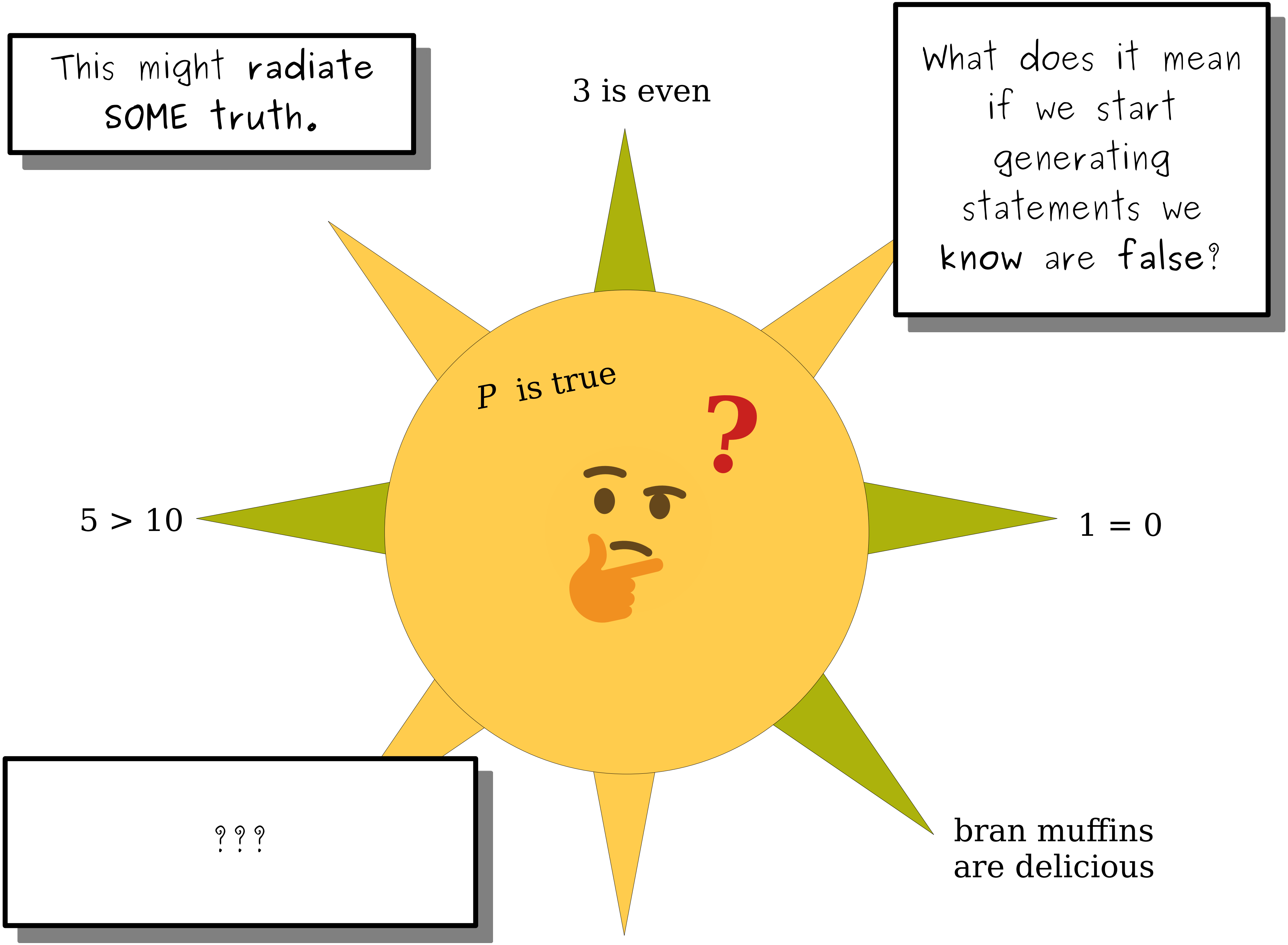
This might radiate **SOME truth.**



What does it mean if we start generating statements we **know** are **false**?

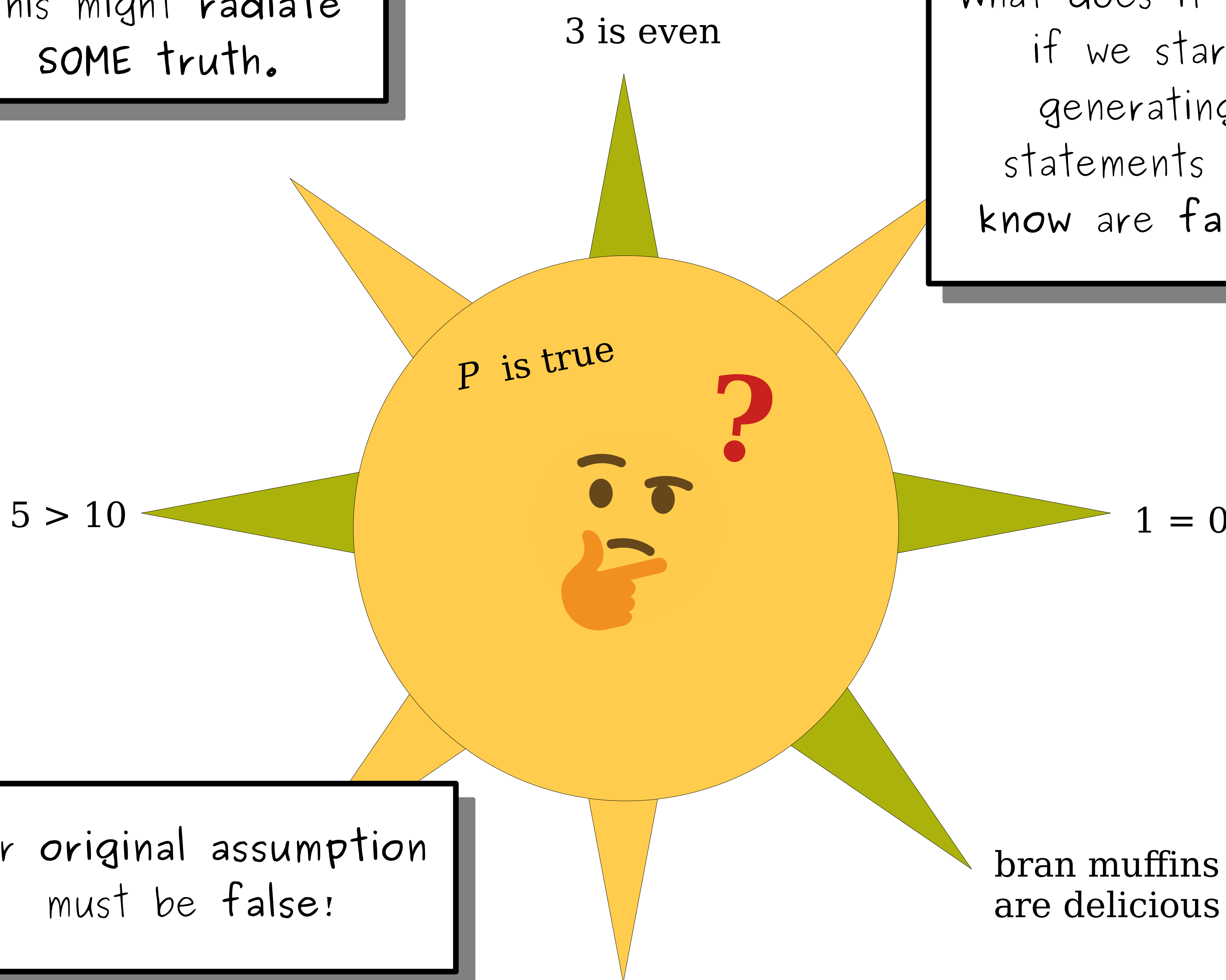

This might radiate SOME truth.
What does it mean if we start generating statements we know are false?
3 is even
P is true
?
5 > 10
1 = 0


This might radiate SOME truth.
What does it mean if we start generating statements we know are false?
3 is even
P is true
?
5 > 10
1 = 0
bran muffins are delicious

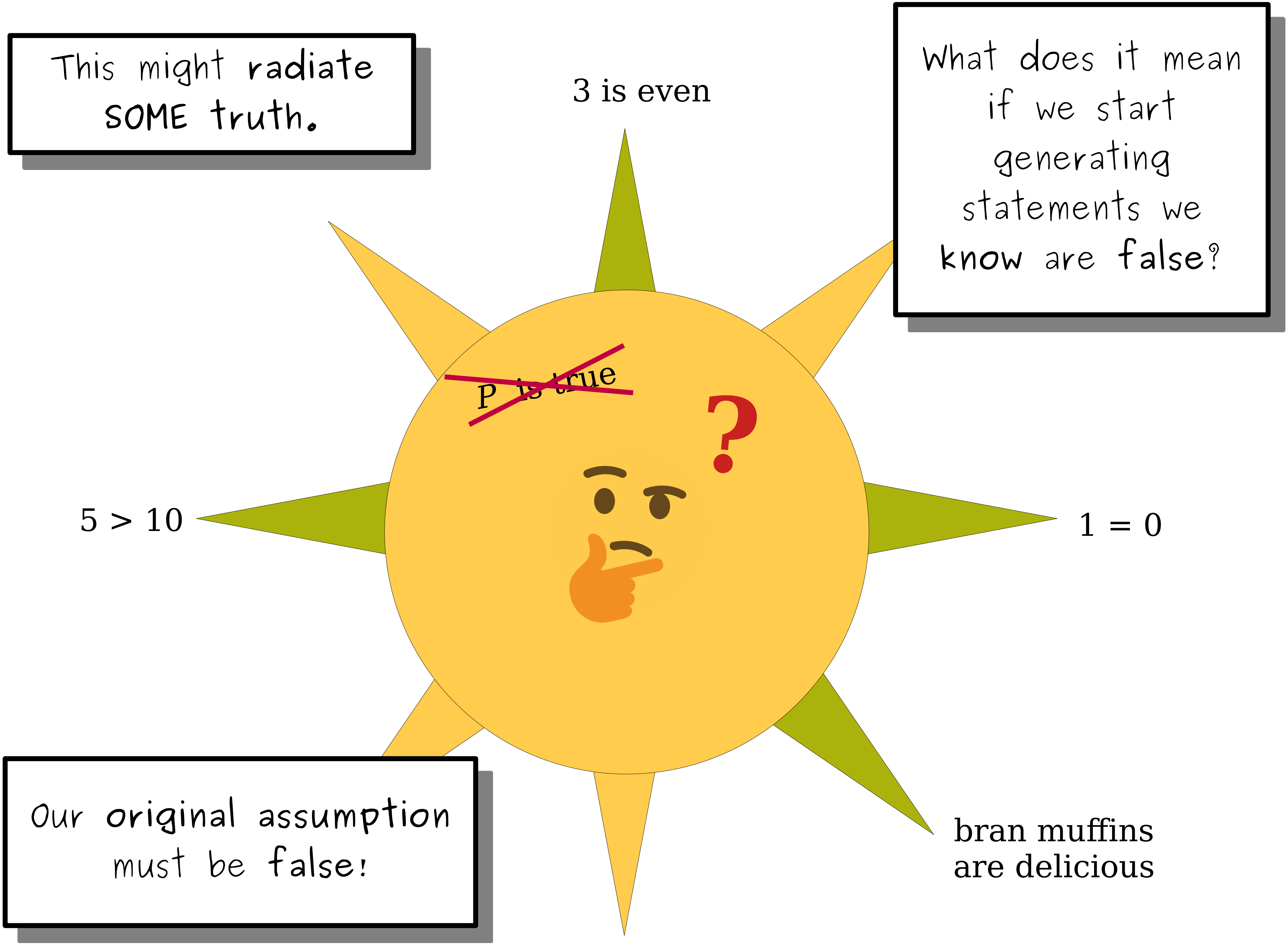

This might radiate SOME truth.
What does it mean if we start generating statements we know are false?
3 is even
P is true
5 > 10
1 = 0
bran muffins are delicious
???

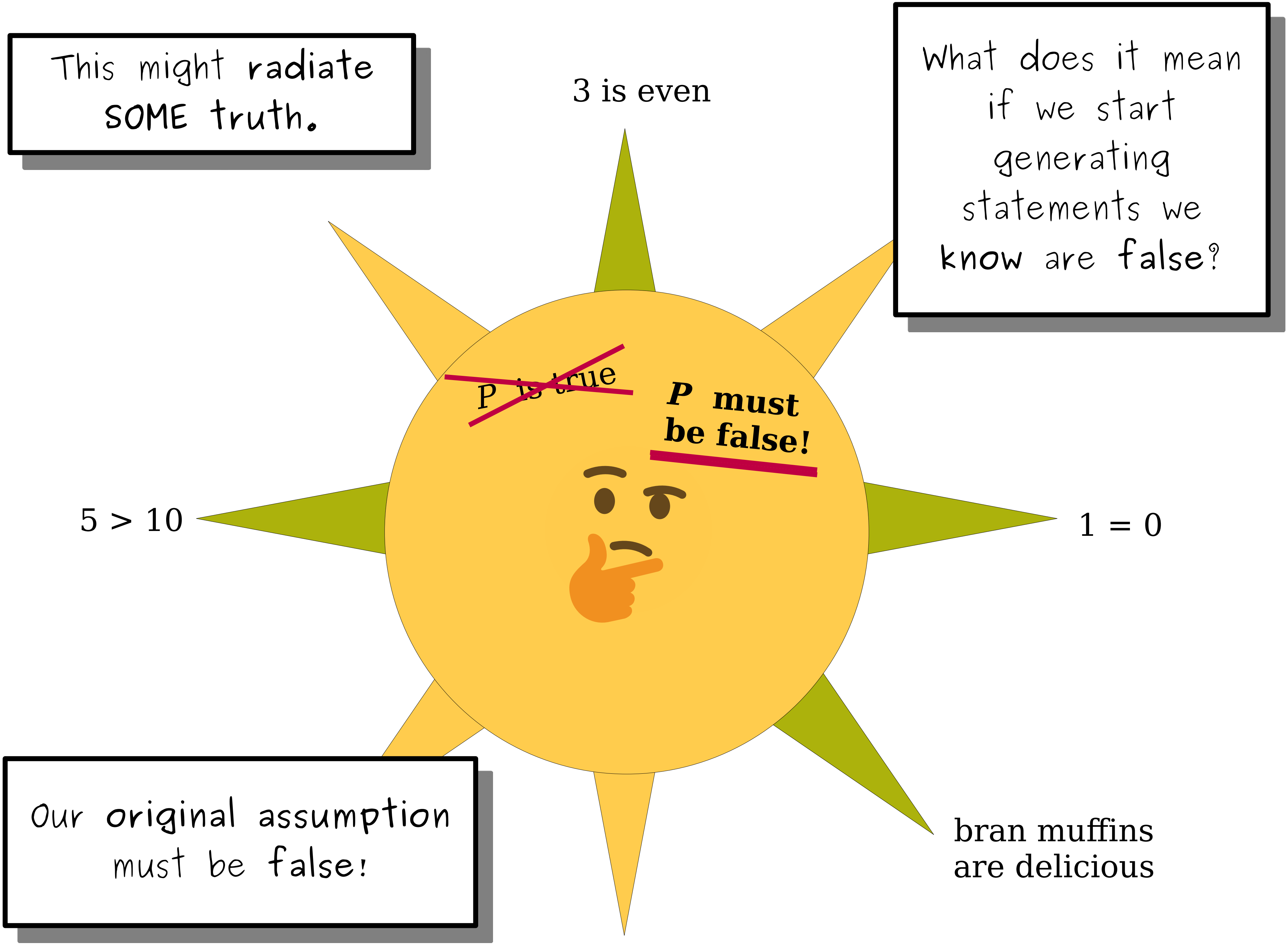
This might radiate **SOME** truth.

What does it mean if we start generating statements we **know** are **false**?



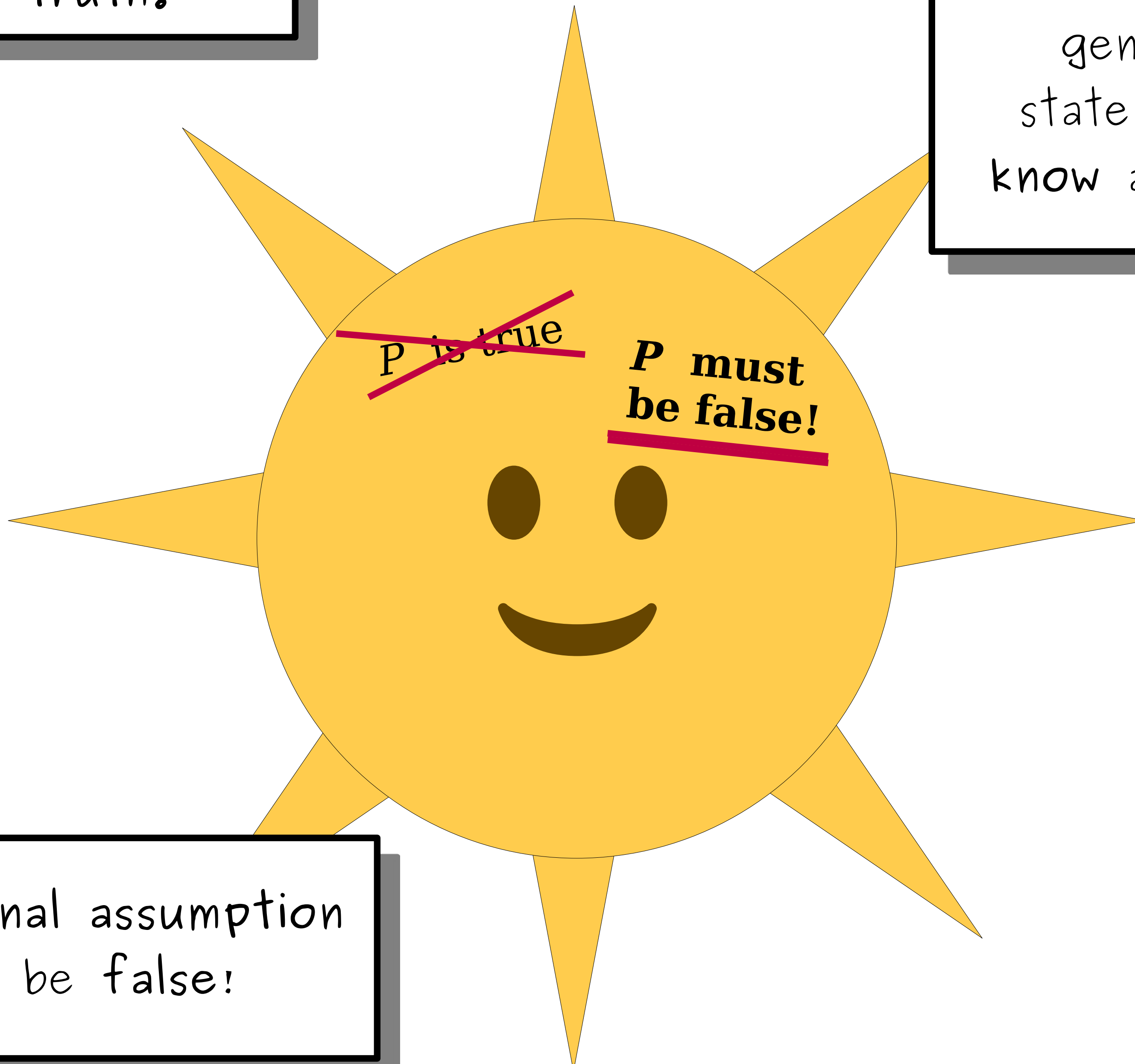
Our **original** assumption must be **false**!


This might radiate SOME truth.
What does it mean if we start generating statements we know are false?
3 is even
P is true
?
5 > 10
1 = 0
bran muffins are delicious
Our original assumption must be false!


This might radiate SOME truth.
What does it mean if we start generating statements we know are false?
3 is even
P is true
P must be false!
5 > 10
1 = 0
bran muffins are delicious
Our original assumption must be false!

This might radiate SOME truth.

What does it mean if we start generating statements we know are false?



Our original assumption must be false!

This gives rise to a powerful proof technique called **proof by contradiction**!

Suppose we want to use this technique to show that $\boldsymbol{P}$ is **true**.

Suppose we want to use this technique to show that $\boldsymbol{P}$ is **true**.

What proposition can we place in the Zone of Uncertainty to accomplish this?

Suppose we want to use this technique to show that ***P*** is **true**.

What proposition can we place in the Zone of Uncertainty to accomplish this?

Answer:

Suppose we want to use this technique to show that P is **true**.

What proposition can we place in the Zone of Uncertainty to accomplish this?

Answer: The negation of P !

Suppose we want to use this technique to show that $\boldsymbol{P}$ is **true**.

What proposition can we place in the Zone of Uncertainty to accomplish this?

Answer: The negation of $\boldsymbol{P}$!

Suppose we want to use this technique to show that $\boldsymbol{P}$ is **true**.

What proposition can we place in the Zone of Uncertainty to accomplish this?

Answer: The negation of $\boldsymbol{P}$!

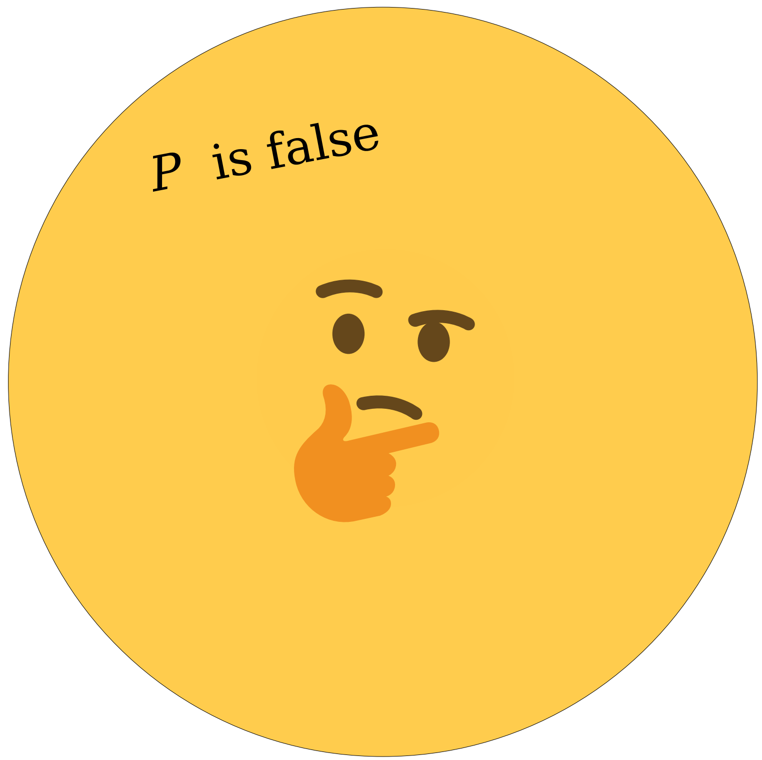
i.e., $\boldsymbol{P}$ is **false**

Suppose we want to use this technique to show that ***P*** is **true**.

What proposition can we place in the Zone of Uncertainty to accomplish this?

Answer: The negation of ***P*** !

i.e., ***P*** is **false**

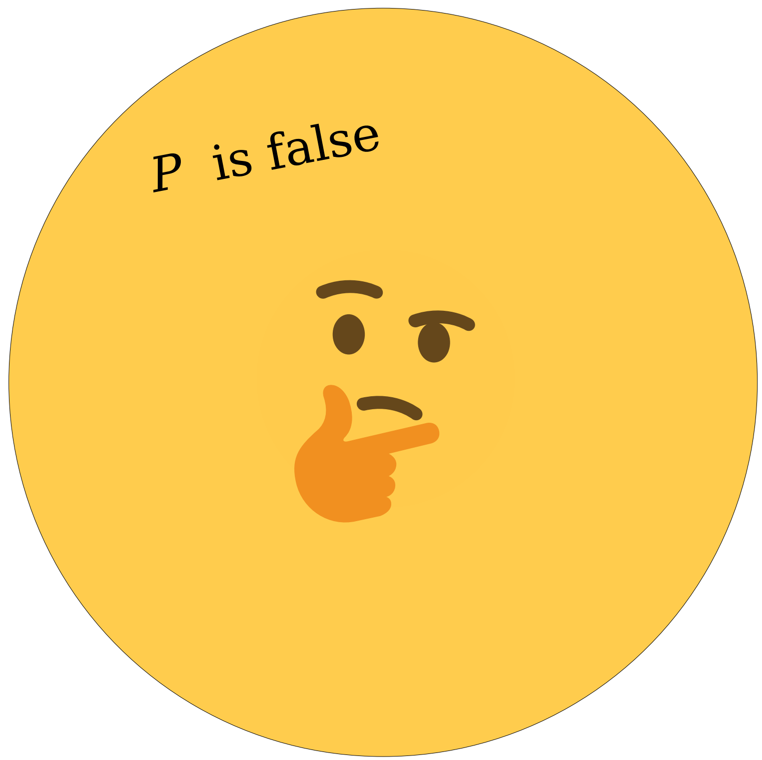


Suppose we want to use this technique to show that $\boldsymbol{P}$ is **true**.

What proposition can we place in the Zone of Uncertainty to accomplish this?

Answer: The negation of $\boldsymbol{P}$!

i.e., $\boldsymbol{P}$ is **false**



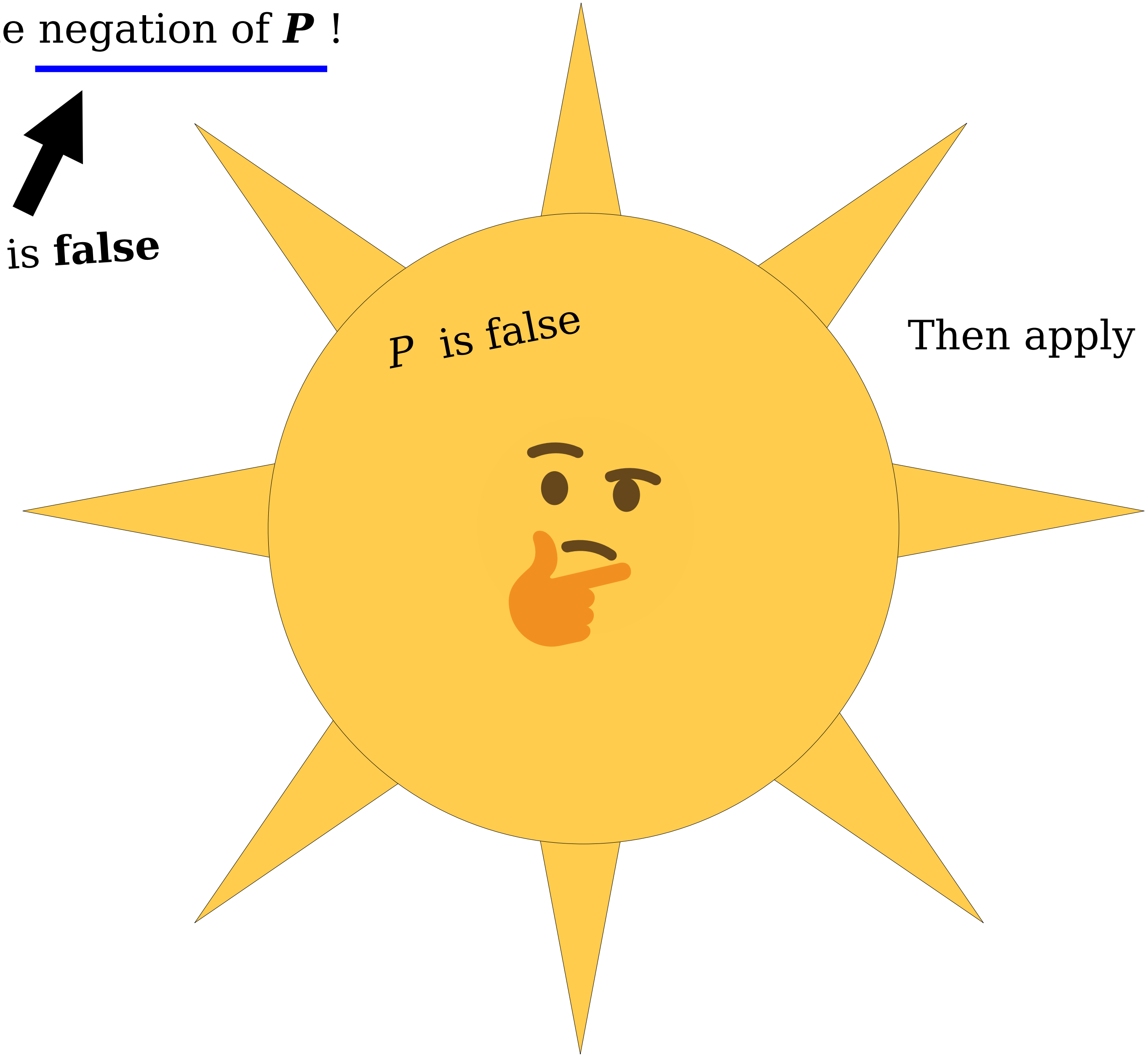
Then apply sound logic...

Suppose we want to use this technique to show that $\boldsymbol{P}$ is **true**.

What proposition can we place in the Zone of Uncertainty to accomplish this?

Answer: The negation of $\boldsymbol{P}$!

i.e., $\boldsymbol{P}$ is **false**



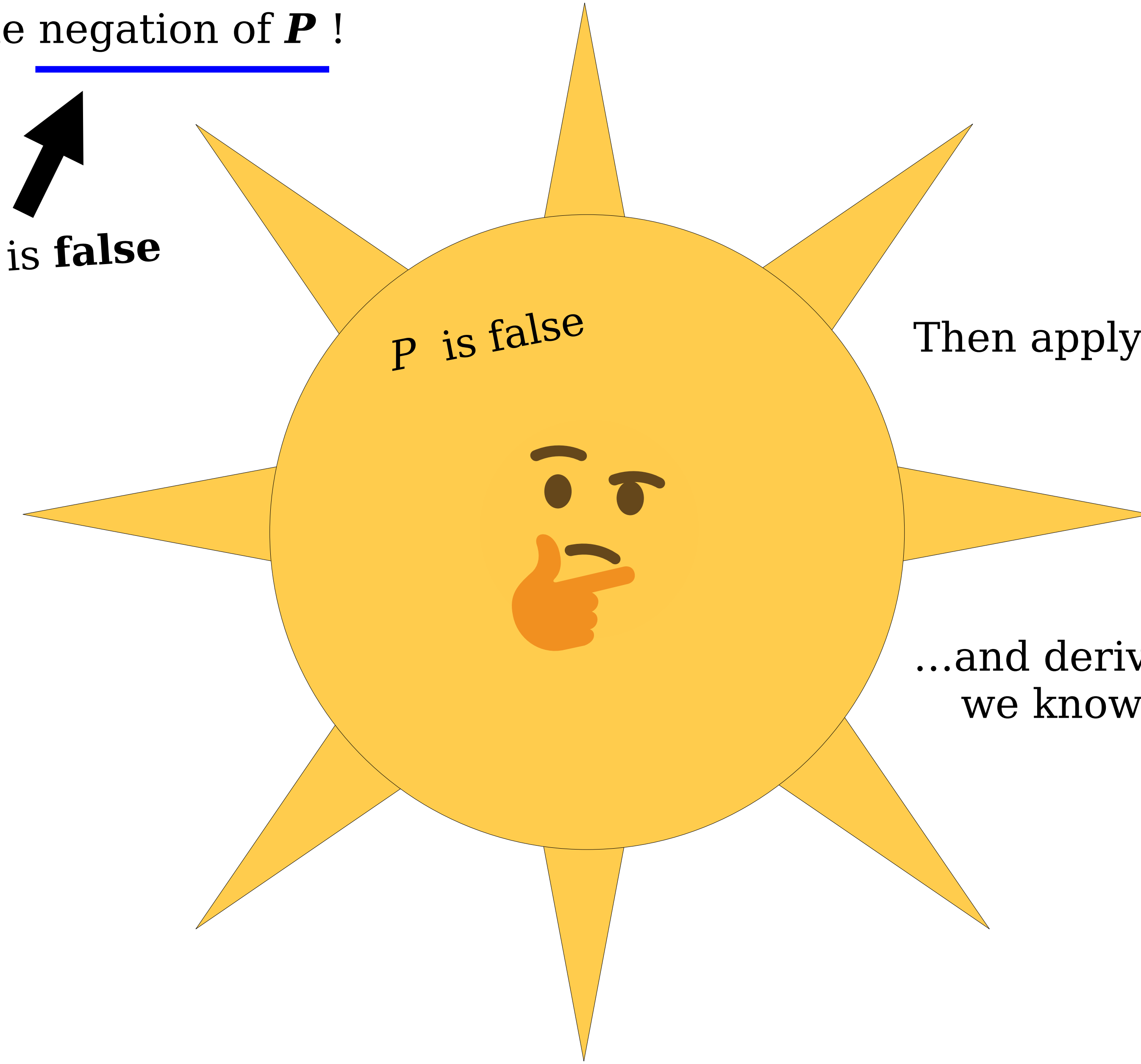
Then apply sound logic...

Suppose we want to use this technique to show that ***P*** is **true**.

What proposition can we place in the Zone of Uncertainty to accomplish this?

Answer: The negation of ***P*** !

i.e., ***P*** is **false**



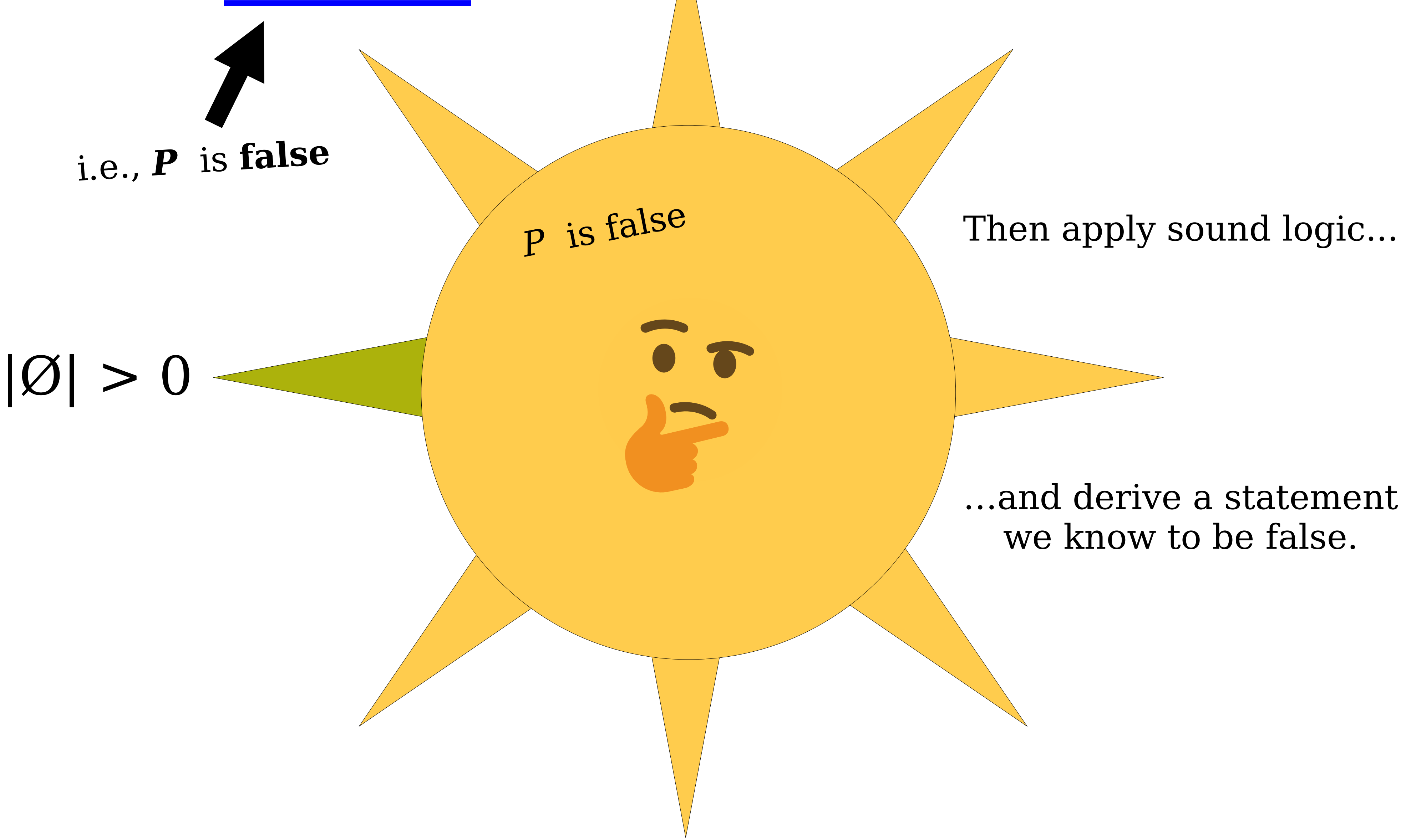
Then apply sound logic...

...and derive a statement we know to be false.

Suppose we want to use this technique to show that ***P*** is **true**.

What proposition can we place in the Zone of Uncertainty to accomplish this?

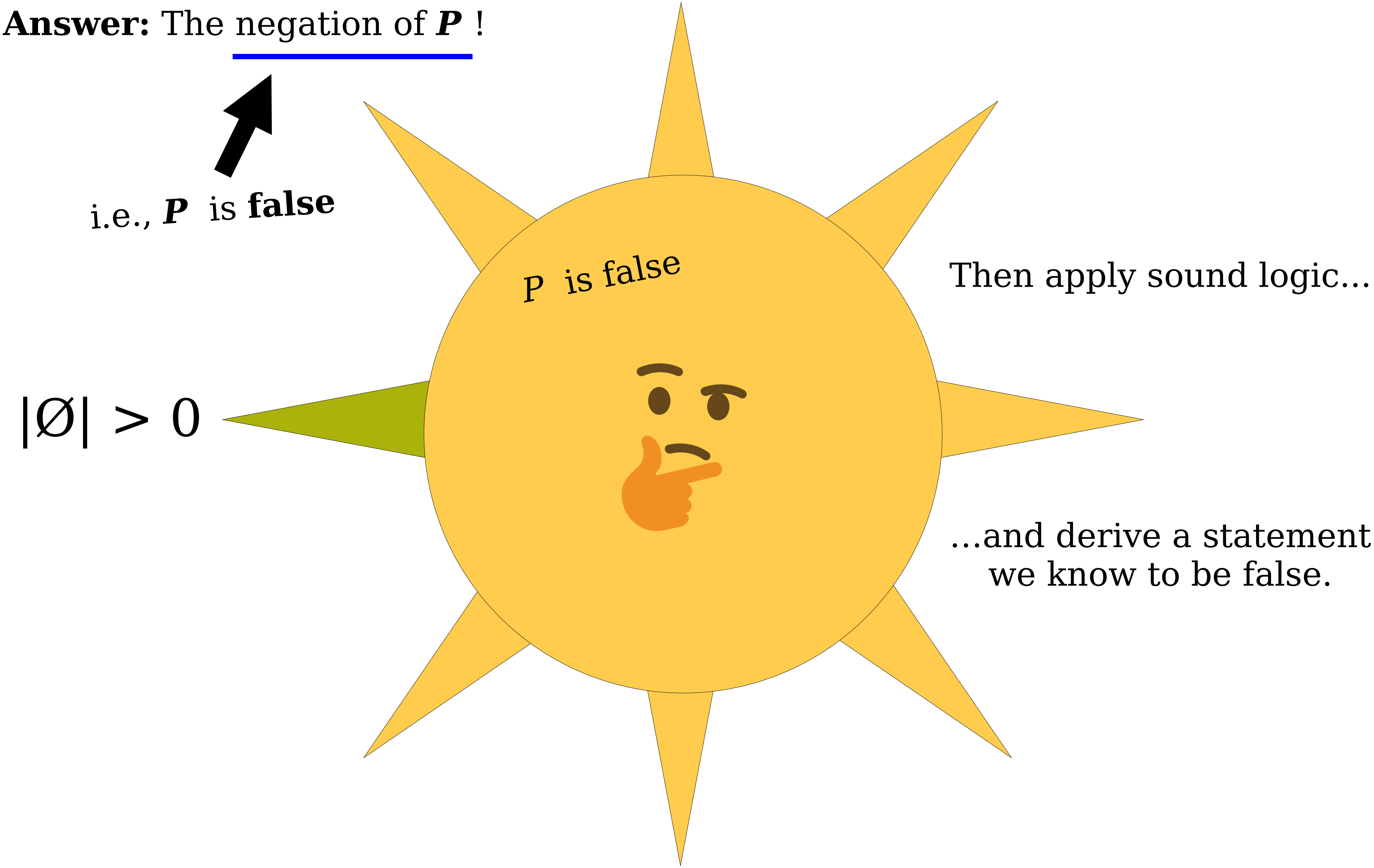
Answer: The negation of ***P*** !



Suppose we want to use this technique to show that ***P*** is **true**.

What proposition can we place in the Zone of Uncertainty to accomplish this?

Answer: The negation of ***P*** !



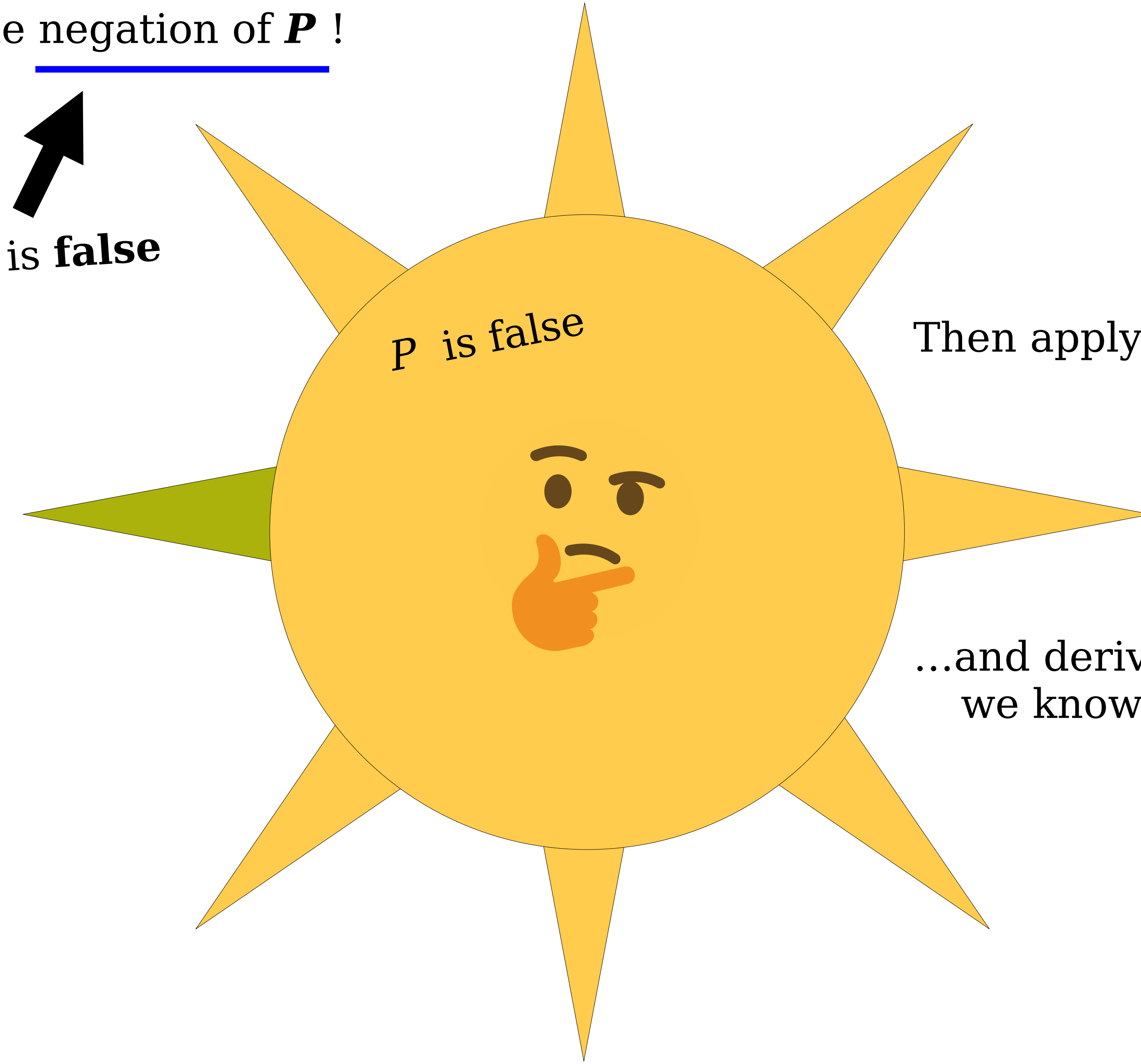
Suppose we want to use this technique to show that ***P*** is **true**.

What proposition can we place in the Zone of Uncertainty to accomplish this?

Answer: The negation of ***P*** !

i.e., ***P*** is **false**

$|\varnothing| > 0$



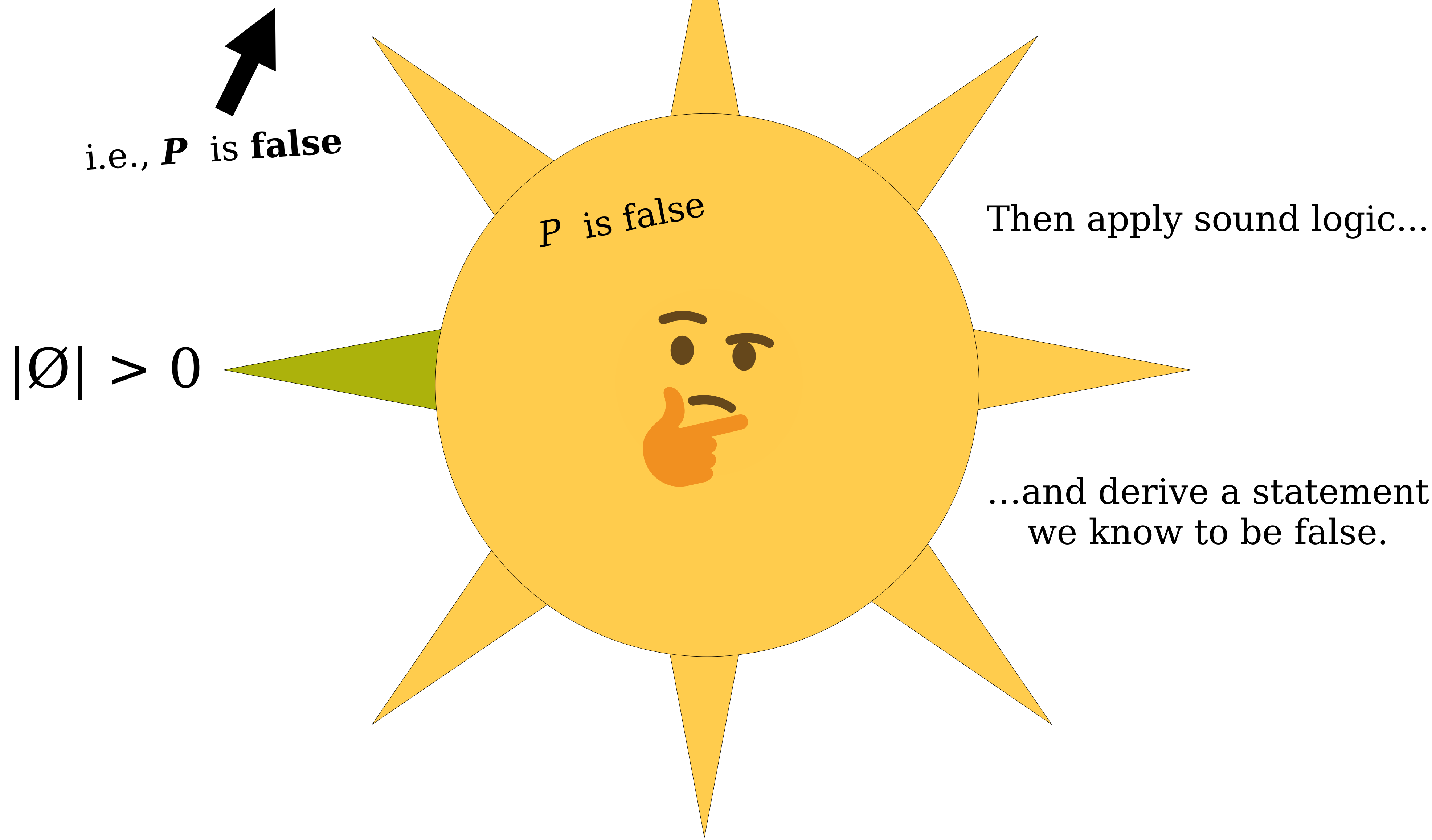
Then apply sound logic…

…and derive a statement we know to be false.

Suppose we want to use this technique to show that ***P*** is **true**.

What proposition can we place in the Zone of Uncertainty to accomplish this?

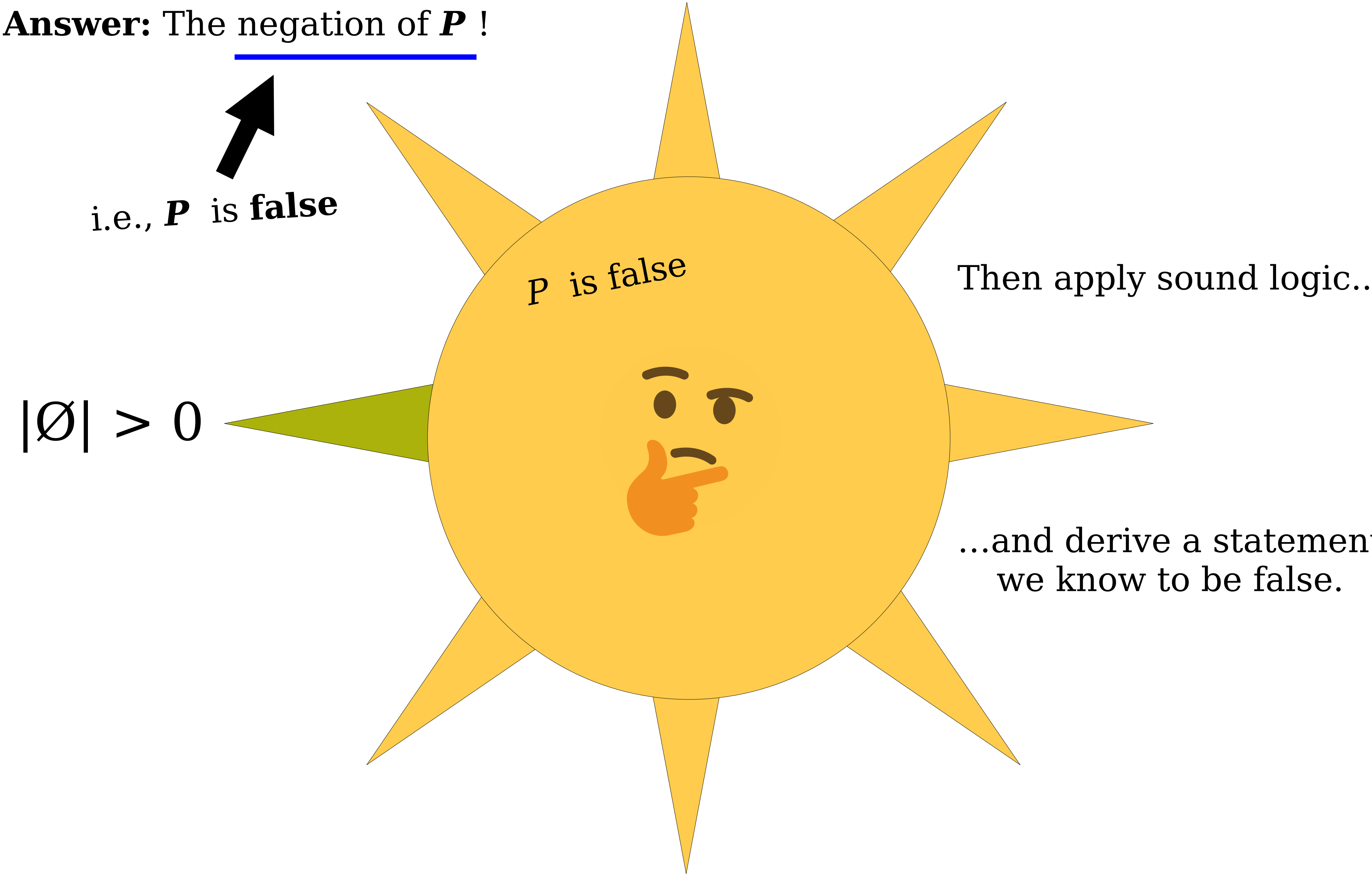
Answer: The negation of ***P*** !



Suppose we want to use this technique to show that ***P*** is **true**.

What proposition can we place in the Zone of Uncertainty to accomplish this?

Answer: The negation of ***P*** !



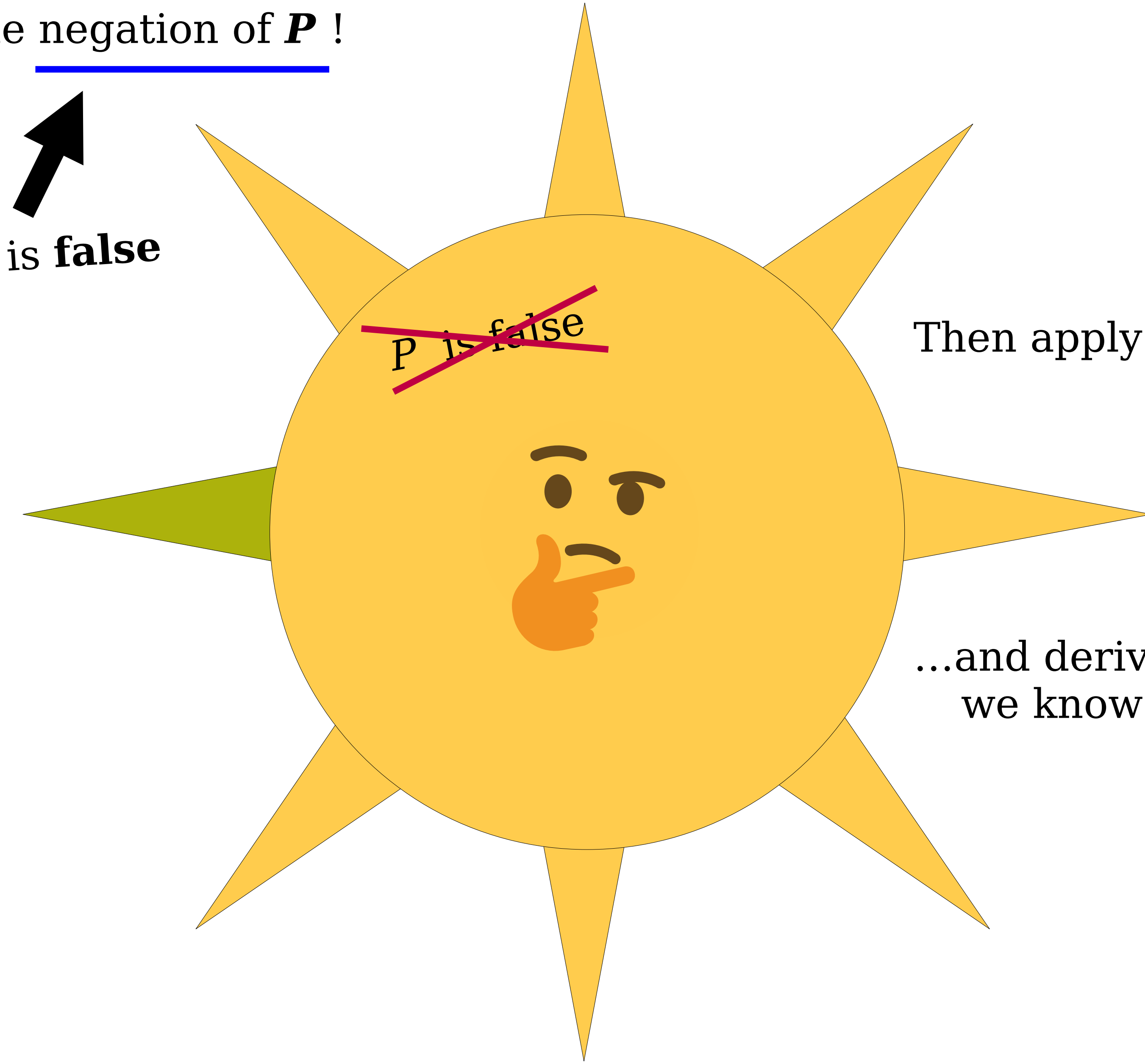
Suppose we want to use this technique to show that ***P*** is **true**.

What proposition can we place in the Zone of Uncertainty to accomplish this?

Answer: The negation of ***P*** !

i.e., ***P*** is **false**

$|\varnothing| > 0$



Then apply sound logic...

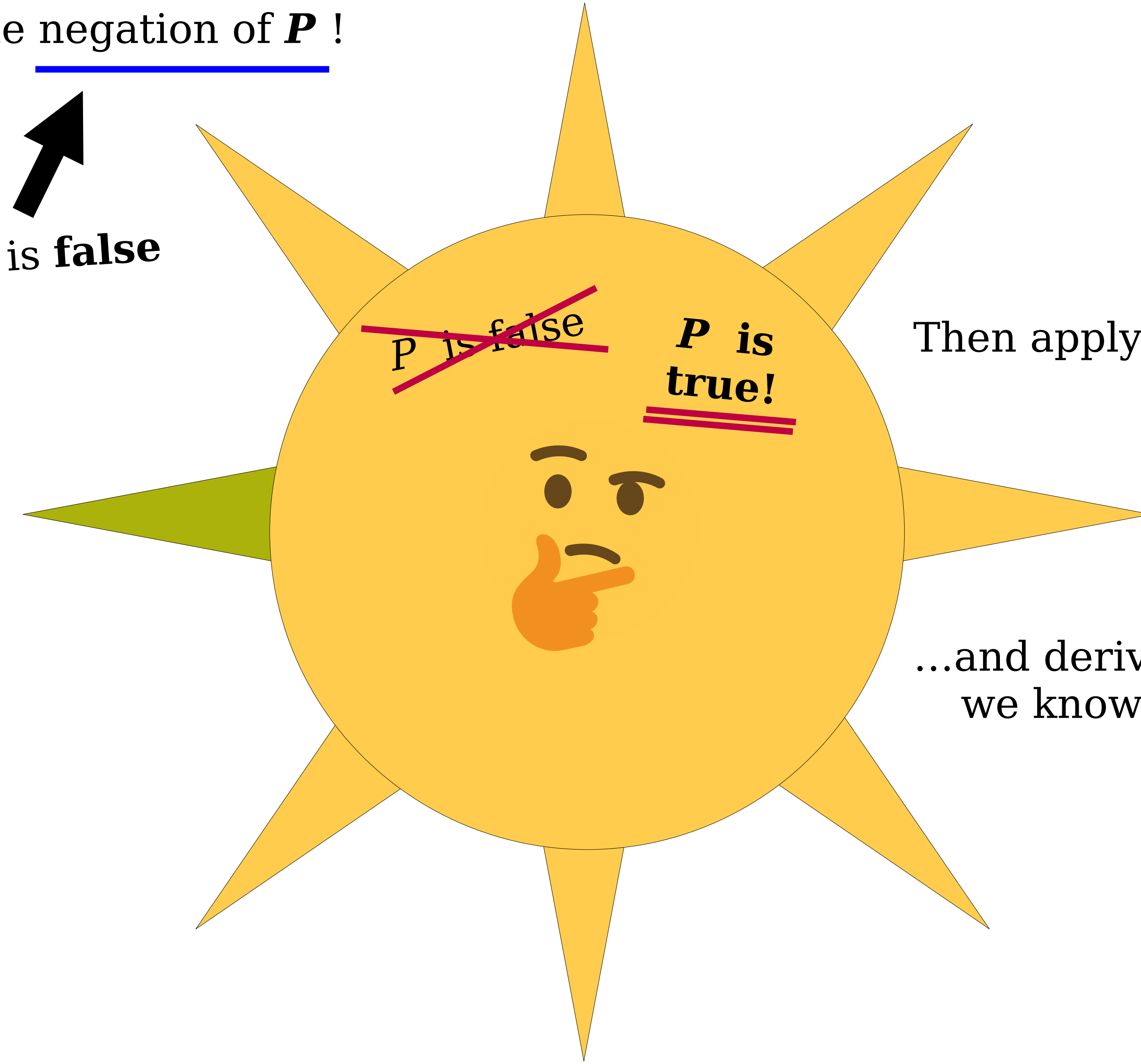
...and derive a statement we know to be false.

Suppose we want to use this technique to show that ***P*** is **true**.

What proposition can we place in the Zone of Uncertainty to accomplish this?

Answer: The negation of ***P*** !

i.e., ***P*** is **false**



$|\varnothing| > 0$

Then apply sound logic…

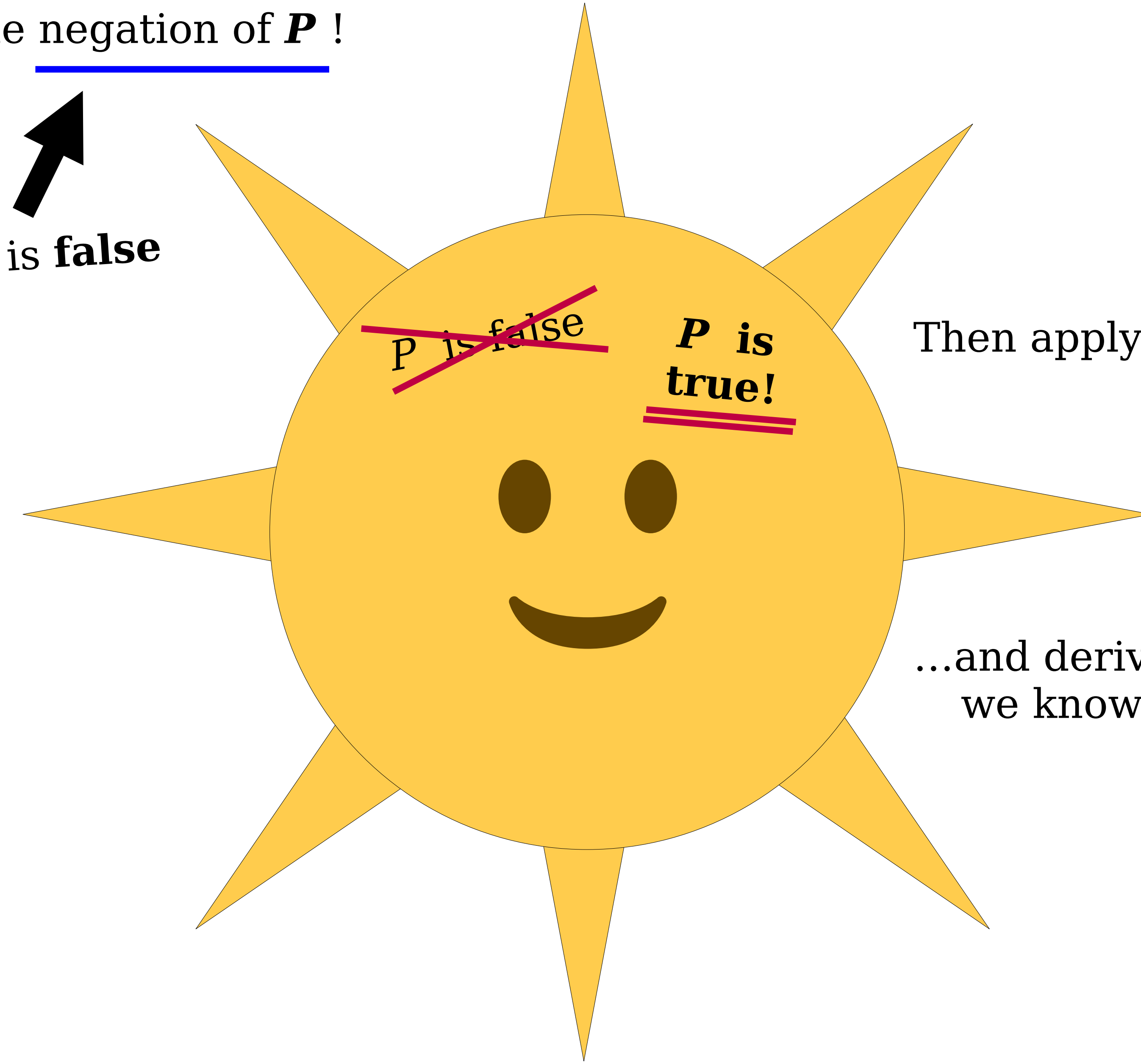
…and derive a statement we know to be false.

Suppose we want to use this technique to show that ***P*** is **true**.

What proposition can we place in the Zone of Uncertainty to accomplish this?

Answer: The negation of ***P*** !

i.e., ***P*** is **false**



Then apply sound logic…

…and derive a statement we know to be false.

Summary: Proof by Contradiction

- ***Key Idea:*** Prove a statement P is true by showing that it isn't false.
- First, assume that P is false. The goal is to show that this assumption is silly.
- Next, show this leads to an impossible result.
  - For example, we might have that $1 = 0$, that $x \in S$ and $x \notin S$, that a number is both even and odd, etc.
- Finally, conclude that since P can't be false, we know that P must be true.

An Example: ***Set Cardinalities***

Set Cardinalities

- We've seen sets of many different cardinalities:
  - $|\emptyset| = 0$
  - $|\{1, 2, 3\}| = 3$
  - $|\{ n \in \mathbb{N} \mid n < 137 \}| = 137$
  - $|\mathbb{N}| = \aleph_0$.
  - $|\wp(\mathbb{N})| > |\mathbb{N}|$
- These span from the finite up through the infinite.
- ***Question:*** Is there a "largest" set? That is, is there a set that's bigger than every other set?

Theorem: There is no largest set.

Theorem: There is no largest set.

Proof:

Theorem: There is no largest set.

Proof:

To prove this statement by contradiction, we're going to assume its negation.

Theorem: There is no largest set.

Proof:

To prove this statement by contradiction, we're going to assume its negation.

What is the negation of the statement "there is no largest set?"

Theorem: There is no largest set.

Proof:

To prove this statement by contradiction, we're going to assume its negation.

What is the negation of the statement "there is no largest set?"

One option: "there *is* a largest set."

Theorem: There is no largest set.

Proof: Assume for the sake of contradiction that there is a largest set; call it S.

To prove this statement by contradiction, we're going to assume its negation.

What is the negation of the statement "there is no largest set?"

One option: "there *is* a largest set."

Theorem: There is no largest set.

Proof: Assume for the sake of contradiction that there is a largest set; call it S.

Theorem: There is no largest set.

Proof: Assume for the sake of contradiction that there is a largest set; call it S.

Theorem: There is no largest set.

Proof: Assume for the sake of contradiction that there is a largest set; call it S.

Notice that we're announcing

1. that this is a proof by contradiction, and
2. what, specifically, we're assuming.

This helps the reader understand where we're going. Remember – proofs are meant to be read by other people!

Theorem: There is no largest set.

Proof: Assume for the sake of contradiction that there is a largest set; call it S.

Theorem: There is no largest set.

Proof: Assume for the sake of contradiction that there is a largest set; call it S.

Now, consider the set $\wp(S)$.

Theorem: There is no largest set.

Proof: Assume for the sake of contradiction that there is a largest set; call it S.

Now, consider the set $\wp(S)$. By Cantor's Theorem, we know that $|S| < |\wp(S)|$, so $\wp(S)$ is a larger set than S.

Theorem: There is no largest set.

Proof: Assume for the sake of contradiction that there is a largest set; call it S.

Now, consider the set $\wp(S)$. By Cantor's Theorem, we know that $|S| < |\wp(S)|$, so $\wp(S)$ is a larger set than S. This contradicts the fact that S is the largest set.

Theorem: There is no largest set.

Proof: Assume for the sake of contradiction that there is a largest set; call it S.

Now, consider the set $\wp(S)$. By Cantor's Theorem, we know that $|S| < |\wp(S)|$, so $\wp(S)$ is a larger set than S. This contradicts the fact that S is the largest set.

We've reached a contradiction, so our assumption must have been wrong.

Theorem: There is no largest set.

Proof: Assume for the sake of contradiction that there is a largest set; call it S.

Now, consider the set $\wp(S)$. By Cantor's Theorem, we know that $|S| < |\wp(S)|$, so $\wp(S)$ is a larger set than S. This contradicts the fact that S is the largest set.

We've reached a contradiction, so our assumption must have been wrong. Therefore, there is no largest set.

Theorem: There is no largest set.

Proof: Assume for the sake of contradiction that there is a largest set; call it S.

Now, consider the set $\wp(S)$. By Cantor's Theorem, we know that $|S| < |\wp(S)|$, so $\wp(S)$ is a larger set than S. This contradicts the fact that S is the largest set.

We've reached a contradiction, so our assumption must have been wrong. Therefore, there is no largest set. ■

Theorem: There is no largest set.

Proof: Assume for the sake of contradiction that there is a largest set; call it S.

Now, consider the set $\wp(S)$. By Cantor's Theorem, we know that $|S| < |\wp(S)|$, so $\wp(S)$ is a larger set than S. This contradicts the fact that S is the largest set.

We've reached a contradiction, so our assumption must have been wrong. Therefore, there is no largest set. ■

Theorem: There is no largest set.

Proof: Assume for the sake of contradiction that there is a largest set; call it S.

The three key pieces:

1. Say that the proof is by contradiction.
2. Say what you are assuming is the negation of the statement to prove.
3. Say you have reached a contradiction and what the contradiction means.

In CS103, please include all these steps in your proofs!

We've reached a contradiction, so our assumption must have been wrong. Therefore, there is no largest set. ■

Theorem: There is no largest set.

Proof: Assume for the sake of contradiction that there is a largest set; call it S.

Now, consider the set $\wp(S)$. By Cantor's Theorem, we know that $|S| < |\wp(S)|$, so $\wp(S)$ is a larger set than S. This contradicts the fact that S is the largest set.

We've reached a contradiction, so our assumption must have been wrong. Therefore, there is no largest set. ■

Another Example

Latin Squares

- A ***Latin square*** is an $n \times n$ grid filled with the numbers 1, 2, …, n such that every number appears in each row and each column exactly once.

1	2	3
2	3	1
3	1	2

1	3	4	2
4	2	1	3
2	1	3	4
3	4	2	1

1	3	5	2	4
3	1	4	5	2
4	5	2	3	1
5	2	1	4	3
2	4	3	1	5

3	2	1	4	5	6
2	4	6	1	3	5
5	6	4	3	2	1
4	1	5	2	6	3
6	3	2	5	1	4
1	5	3	6	4	2

Latin Squares

- A ***Latin square*** is an $n \times n$ grid filled with the numbers 1, 2, …, n such that every number appears in each row and each column exactly once.
- The ***main diagonal*** of a Latin square runs from the top-left corner to the bottom-right corner.

1	2	3
2	3	1
3	1	2

1	3	4	2
4	2	1	3
2	1	3	4
3	4	2	1

1	3	5	2	4
3	1	4	5	2
4	5	2	3	1
5	2	1	4	3
2	4	3	1	5

3	2	1	4	5	6
2	4	6	1	3	5
5	6	4	3	2	1
4	1	5	2	6	3
6	3	2	5	1	4
1	5	3	6	4	2

Latin Squares

- A ***Latin square*** is an $n \times n$ grid filled with the numbers 1, 2, …, n such that every number appears in each row and each column exactly once.
- The ***main diagonal*** of a Latin square runs from the top-left corner to the bottom-right corner.
- A Latin square is ***symmetric*** if the numbers are symmetric across the main diagonal.

1	2	3
2	3	1
3	1	2

1	3	4	2
4	2	1	3
2	1	3	4
3	4	2	1

1	3	5	2	4
3	1	4	5	2
4	5	2	3	1
5	2	1	4	3
2	4	3	1	5

3	2	1	4	5	6
2	4	6	1	3	5
5	6	4	3	2	1
4	1	5	2	6	3
6	3	2	5	1	4
1	5	3	6	4	2

Latin Squares

- A ***Latin square*** is an $n \times n$ grid filled with the numbers 1, 2, …, n such that every number appears in each row and each column exactly once.
- The ***main diagonal*** of a Latin square runs from the top-left corner to the bottom-right corner.
- A Latin square is ***symmetric*** if the numbers are symmetric across the main diagonal.

1	2	3
2	3	1
3	1	2

1	2	3	4	5
2	5	4	1	3
3	4	2	5	1
4	1	5	3	2
5	3	1	2	4

3	2	5	1	4
2	1	4	5	3
5	4	2	3	1
1	5	3	4	2
4	3	1	2	5

2	5	1	4	3
5	1	3	2	4
1	3	4	5	2
4	2	5	3	1
3	4	2	1	5

Latin Squares

- Notice anything about what's on the main diagonals of these symmetric Latin squares?
- ***Theorem:*** Every odd-sized symmetric Latin square has every number 1, 2, …, n on its main diagonal.

1	2	3
2	3	1
3	1	2

1	2	3	4	5
2	5	4	1	3
3	4	2	5	1
4	1	5	3	2
5	3	1	2	4

3	2	5	1	4
2	1	4	5	3
5	4	2	3	1
1	5	3	4	2
4	3	1	2	5

2	5	1	4	3
5	1	3	2	4
1	3	4	5	2
4	2	5	3	1
3	4	2	1	5

Theorem: Every symmetric Latin square of odd size $n \times n$ has each of the numbers $1, 2, \ldots, n$ on its main diagonal.

Theorem: Every symmetric Latin square of odd size $n \times n$ has each of the numbers $1, 2, \ldots, n$ on its main diagonal.

Proof:

Theorem: Every symmetric Latin square of odd size $n \times n$ has each of the numbers 1, 2, …, n on its main diagonal.

Proof:

What is the negation of the theorem?

Every symmetric Latin square of odd size n × n has each of the numbers 1, 2, …, n on its main diagonal.

Theorem: Every symmetric Latin square of odd size $n \times n$ has each of the numbers 1, 2, …, n on its main diagonal.

Proof:

What is the negation of the theorem?

Every symmetric Latin square of odd size n × n has each of the numbers 1, 2, …, n on its main diagonal.

Theorem: Every symmetric Latin square of odd size $n \times n$ has each of the numbers 1, 2, …, n on its main diagonal.

Proof:

What is the negation of the theorem?

Every symmetric Latin square of odd size n × n has each of the numbers 1, 2, …, n on its main diagonal.

One option:

There is a symmetric Latin square of odd size n × n that does not have one of the numbers 1, 2, …, n on its main diagonal.

Theorem: Every symmetric Latin square of odd size $n \times n$ has each of the numbers 1, 2, …, n on its main diagonal.

Proof: Assume for the sake of contradiction that there is a symmetric Latin square of odd size $n \times n$ that does not have one of the numbers 1, 2, 3, …, n on its main diagonal.

Theorem: Every symmetric Latin square of odd size $n \times n$ has each of the numbers 1, 2, …, n on its main diagonal.

Proof: Assume for the sake of contradiction that there is a symmetric Latin square of odd size $n \times n$ that does not have one of the numbers 1, 2, 3, …, n on its main diagonal.

Notice that we're announcing

1. that this is a proof by contradiction, and
2. what, specifically, we're assuming.

This helps the reader understand where we're going. Remember – proofs are meant to be read by other people!

Theorem: Every symmetric Latin square of odd size $n \times n$ has each of the numbers 1, 2, …, n on its main diagonal.

Proof: Assume for the sake of contradiction that there is a symmetric Latin square of odd size $n \times n$ that does not have one of the numbers 1, 2, 3, …, n on its main diagonal.

Theorem: Every symmetric Latin square of odd size $n \times n$ has each of the numbers 1, 2, …, n on its main diagonal.

Proof: Assume for the sake of contradiction that there is a symmetric Latin square of odd size $n \times n$ that does not have one of the numbers 1, 2, 3, …, n on its main diagonal. Call the missing number r.

Theorem: Every symmetric Latin square of odd size $n \times n$ has each of the numbers 1, 2, …, n on its main diagonal.

Proof: Assume for the sake of contradiction that there is a symmetric Latin square of odd size $n \times n$ that does not have one of the numbers 1, 2, 3, …, n on its main diagonal. Call the missing number r.

Let k be the number of times r appears above the main diagonal.

Theorem: Every symmetric Latin square of odd size $n \times n$ has each of the numbers 1, 2, …, n on its main diagonal.

Proof: Assume for the sake of contradiction that there is a symmetric Latin square of odd size $n \times n$ that does not have one of the numbers 1, 2, 3, …, n on its main diagonal. Call the missing number r.

Let k be the number of times r appears above the main diagonal. Since the Latin square is symmetric, there are also k copies of r below the main diagonal.

Theorem: Every symmetric Latin square of odd size $n \times n$ has each of the numbers $1, 2, \ldots, n$ on its main diagonal.

Proof: Assume for the sake of contradiction that there is a symmetric Latin square of odd size $n \times n$ that does not have one of the numbers $1, 2, 3, \ldots, n$ on its main diagonal. Call the missing number r.

Let k be the number of times r appears above the main diagonal. Since the Latin square is symmetric, there are also k copies of r below the main diagonal. And because r doesn't appear on the main diagonal, that accounts for all copies of r, so there are exactly $2k$ copies of r.

Theorem: Every symmetric Latin square of odd size $n \times n$ has each of the numbers 1, 2, …, n on its main diagonal.

Proof: Assume for the sake of contradiction that there is a symmetric Latin square of odd size $n \times n$ that does not have one of the numbers 1, 2, 3, …, n on its main diagonal. Call the missing number r.

Let k be the number of times r appears above the main diagonal. Since the Latin square is symmetric, there are also k copies of r below the main diagonal. And because r doesn't appear on the main diagonal, that accounts for all copies of r, so there are exactly $2k$ copies of r.

Independently, we know that r appears n times in the Latin square, once for each of its n rows.

Theorem: Every symmetric Latin square of odd size $n \times n$ has each of the numbers $1, 2, \ldots, n$ on its main diagonal.

Proof: Assume for the sake of contradiction that there is a symmetric Latin square of odd size $n \times n$ that does not have one of the numbers $1, 2, 3, \ldots, n$ on its main diagonal. Call the missing number r.

Let k be the number of times r appears above the main diagonal. Since the Latin square is symmetric, there are also k copies of r below the main diagonal. And because r doesn't appear on the main diagonal, that accounts for all copies of r, so there are exactly $2k$ copies of r.

Independently, we know that r appears n times in the Latin square, once for each of its n rows.

Combining these results, we see that $n = 2k$.

Theorem: Every symmetric Latin square of odd size $n \times n$ has each of the numbers $1, 2, \ldots, n$ on its main diagonal.

Proof: Assume for the sake of contradiction that there is a symmetric Latin square of odd size $n \times n$ that does not have one of the numbers $1, 2, 3, \ldots, n$ on its main diagonal. Call the missing number r.

Let k be the number of times r appears above the main diagonal. Since the Latin square is symmetric, there are also k copies of r below the main diagonal. And because r doesn't appear on the main diagonal, that accounts for all copies of r, so there are exactly $2k$ copies of r.

Independently, we know that r appears n times in the Latin square, once for each of its n rows.

Combining these results, we see that $n = 2k$. This means that n is even, contradicting the fact that n is odd.

Theorem: Every symmetric Latin square of odd size $n \times n$ has each of the numbers $1, 2, \ldots, n$ on its main diagonal.

Proof: Assume for the sake of contradiction that there is a symmetric Latin square of odd size $n \times n$ that does not have one of the numbers $1, 2, 3, \ldots, n$ on its main diagonal. Call the missing number r.

Let k be the number of times r appears above the main diagonal. Since the Latin square is symmetric, there are also k copies of r below the main diagonal. And because r doesn't appear on the main diagonal, that accounts for all copies of r, so there are exactly $2k$ copies of r.

Independently, we know that r appears n times in the Latin square, once for each of its n rows.

Combining these results, we see that $n = 2k$. This means that n is even, contradicting the fact that n is odd. We've reached a contradiction, so our assumption was wrong.

Theorem: Every symmetric Latin square of odd size $n \times n$ has each of the numbers 1, 2, …, n on its main diagonal.

Proof: Assume for the sake of contradiction that there is a symmetric Latin square of odd size $n \times n$ that does not have one of the numbers 1, 2, 3, …, n on its main diagonal. Call the missing number r.

Let k be the number of times r appears above the main diagonal. Since the Latin square is symmetric, there are also k copies of r below the main diagonal. And because r doesn't appear on the main diagonal, that accounts for all copies of r, so there are exactly $2k$ copies of r.

Independently, we know that r appears n times in the Latin square, once for each of its n rows.

Combining these results, we see that $n = 2k$. This means that n is even, contradicting the fact that n is odd. We've reached a contradiction, so our assumption was wrong. Therefore, all symmetric Latin squares of odd size $n \times n$ have each of the numbers 1, 2, …, and n on their main diagonals.

Theorem: Every symmetric Latin square of odd size $n \times n$ has each of the numbers 1, 2, …, n on its main diagonal.

Proof: Assume for the sake of contradiction that there is a symmetric Latin square of odd size $n \times n$ that does not have one of the numbers 1, 2, 3, …, n on its main diagonal. Call the missing number r.

Let k be the number of times r appears above the main diagonal. Since the Latin square is symmetric, there are also k copies of r below the main diagonal. And because r doesn't appear on the main diagonal, that accounts for all copies of r, so there are exactly $2k$ copies of r.

Independently, we know that r appears n times in the Latin square, once for each of its n rows.

Combining these results, we see that $n = 2k$. This means that n is even, contradicting the fact that n is odd. We've reached a contradiction, so our assumption was wrong. Therefore, all symmetric Latin squares of odd size $n \times n$ have each of the numbers 1, 2, …, and n on their main diagonals. ■

Theorem: Every symmetric Latin square of odd size $n \times n$ has each of the numbers 1, 2, …, n on its main diagonal.

Proof: Assume for the sake of contradiction that there is a symmetric Latin square of odd size $n \times n$ that does not have one of the numbers 1, 2, 3, …, n on its main diagonal. Call the missing number r.

The three key pieces:

1. Say that the proof is by contradiction.
2. Say what you are assuming is the negation of the statement to prove.
3. Say you have reached a contradiction and what the contradiction means.

In CS103, please include all these steps in your proofs!

independently, we know that r appears n times in the Latin square, once for each of its n rows.

Combining these results, we see that $n = 2k$. This means that n is even, contradicting the fact that n is odd. We've reached a contradiction, so our assumption was wrong. Therefore, all symmetric Latin squares of odd size $n \times n$ have each of the numbers 1, 2, …, and n on their main diagonals. ■

(Intermission)

Time-Out for Announcements!

Problem Set One

- Problem Set One goes out today. It’s due next Friday at 1:00PM.
    - Explore the language of set theory and better intuit how it works.
    - Learn more about the structure of mathematical proofs.
    - Write your first “freehand” proofs based on your experiences.
- As always, start early, and reach out if you have any questions!

Office Hours

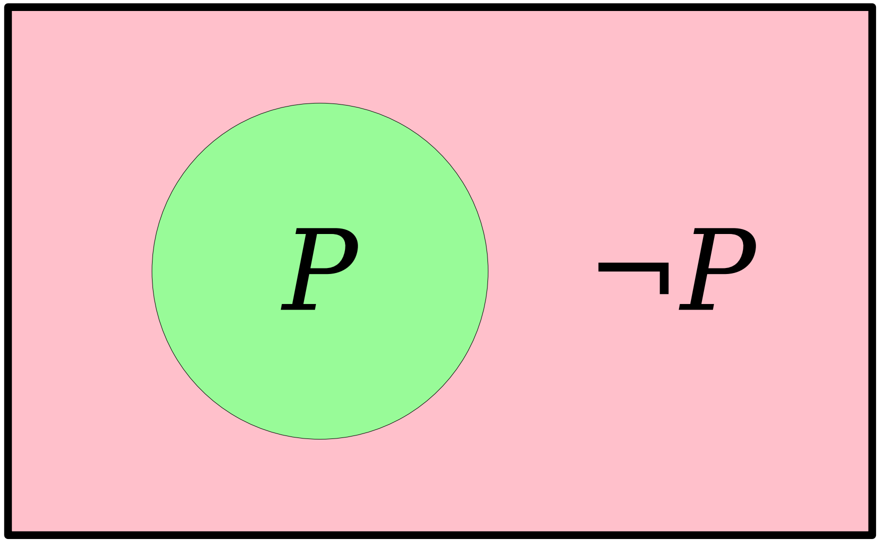
- It is ***completely normal*** in this class to need to get help from time to time.
- Feel free to ask clarifying and conceptual questions on EdStem.
- Need more structured help? We have office hours! Feel free to stop on by.
  - Check out the online “Guide to Office Hours” for more information about how our office hours system works.
  - The OH calendar will soon be available on the course website.
- Office hours start this Sunday.

Readings for Today

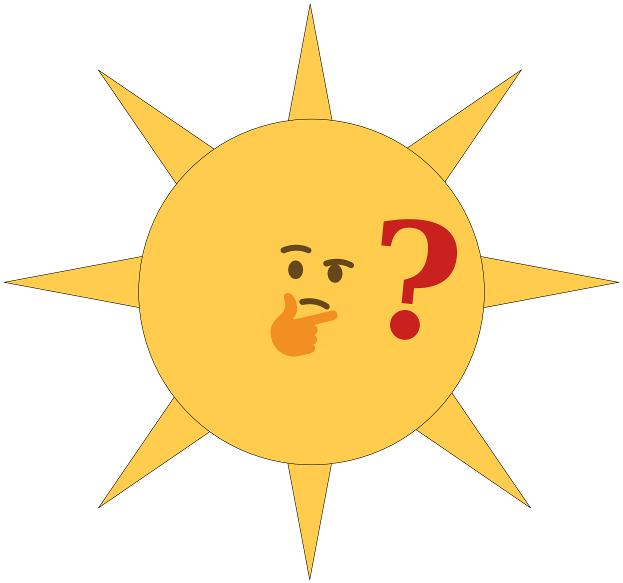
- On the course website we have some information you should look over.
- First is the ***Proofwriting Checklist***. It contains information about style expectations for proofs. We'll be using this when grading, so be sure to read it over.
- Next is the ***Guide to Office Hours***, which talks about how our office hours work and how to make the most effective use of them.
- Finally is the ***Guide to LaTeX***, which explains how to use LaTeX to typeset your problem sets in a way that's so beautiful it will bring tears to your eyes.

(the lights flash in the atrium)

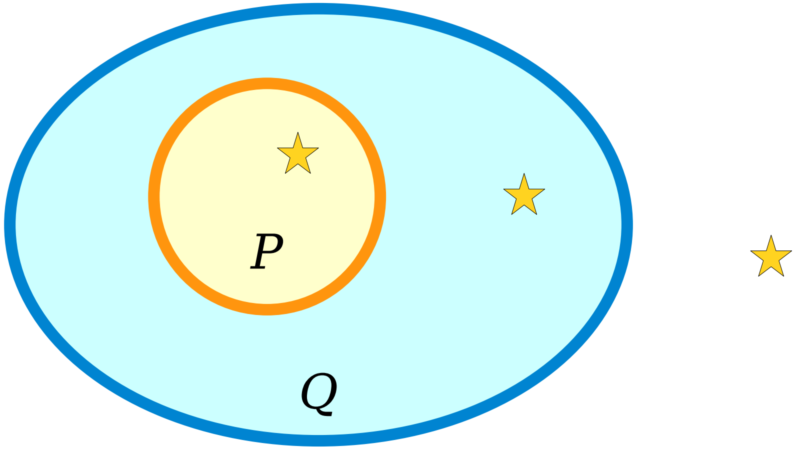
Back to CS103!



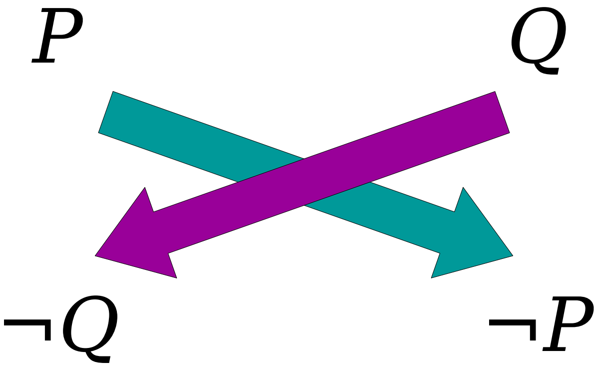
Logical Negation



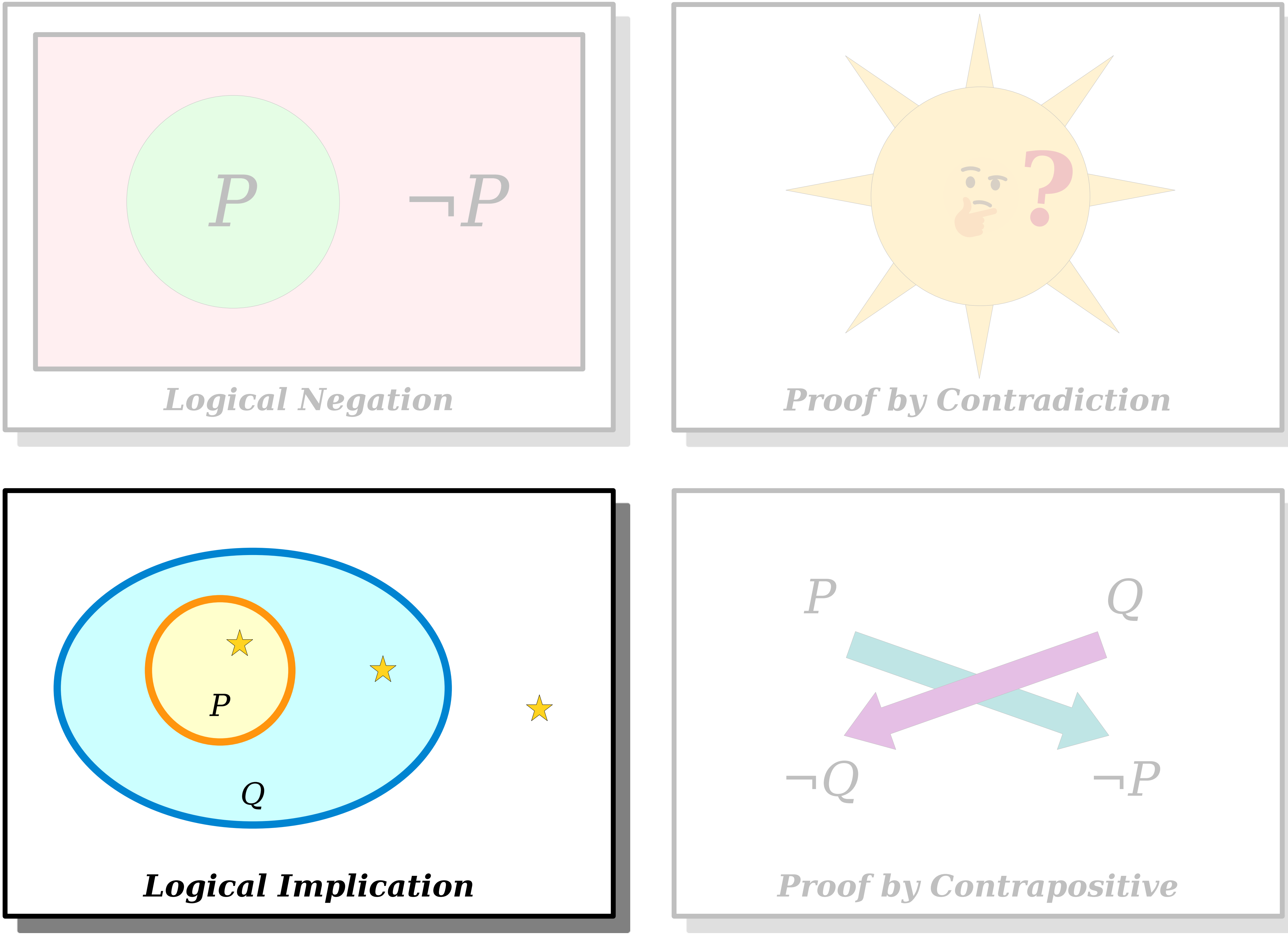
Proof by Contradiction



Logical Implication



Proof by Contrapositive


P
¬P
Logical Negation
?
Proof by Contradiction
P
Q
Logical Implication
P
Q
¬Q
¬P
Proof by Contrapositive

Act III

Logical Implication

If n is an even integer, then n^2 is an even integer.

An ***implication*** is a statement of the form "If P is true, then Q is true."

If n is an even integer, then n^2 is an even integer.

This part of the implication is called the *antecedent*.

This part of the implication is called the *consequent*.

An ***implication*** is a statement of the form "If P is true, then Q is true."

If n is an even integer, then n^2 is an even integer.

An ***implication*** is a statement of the form "If P is true, then Q is true."

If n is an even integer, then n^2 is an even integer.

If m and n are odd integers, then $m+n$ is even.

An ***implication*** is a statement of the form
"If P is true, then Q is true."

If n is an even integer, then n^2 is an even integer.

If m and n are odd integers, then $m+n$ is even.

If you like the way you look that much,
then you should go and love yourself.

An ***implication*** is a statement of the form
"If P is true, then Q is true."

Another Example

If a flying pig bursts into the room and sings a pitch-perfect version of the national anthem, then Sean will throw cookies to the class.

An ***implication*** is a statement of the form "If P is true, then Q is true."

If a flying pig bursts into the room and sings a pitch-perfect version of the national anthem, then Sean will throw cookies to the class.

An ***implication*** is a statement of the form "If P is true, then Q is true."

If a flying pig bursts into the room and sings a pitch-perfect version of the national anthem, then Sean will throw cookies to the class.

An ***implication*** is a statement of the form "If P is true, then Q is true."

If a flying pig bursts into the room and sings a pitch-perfect version of the national anthem, then Sean will throw cookies to the class.

Let's explore the definition and nature of implication through this example!

An ***implication*** is a statement of the form "If P is true, then Q is true."

If a flying pig bursts into the room and sings a pitch-perfect version of the national anthem, then Sean will throw cookies to the class.

Let's explore the definition and nature of implication through this example!

"If ***P***, then ***Q***."

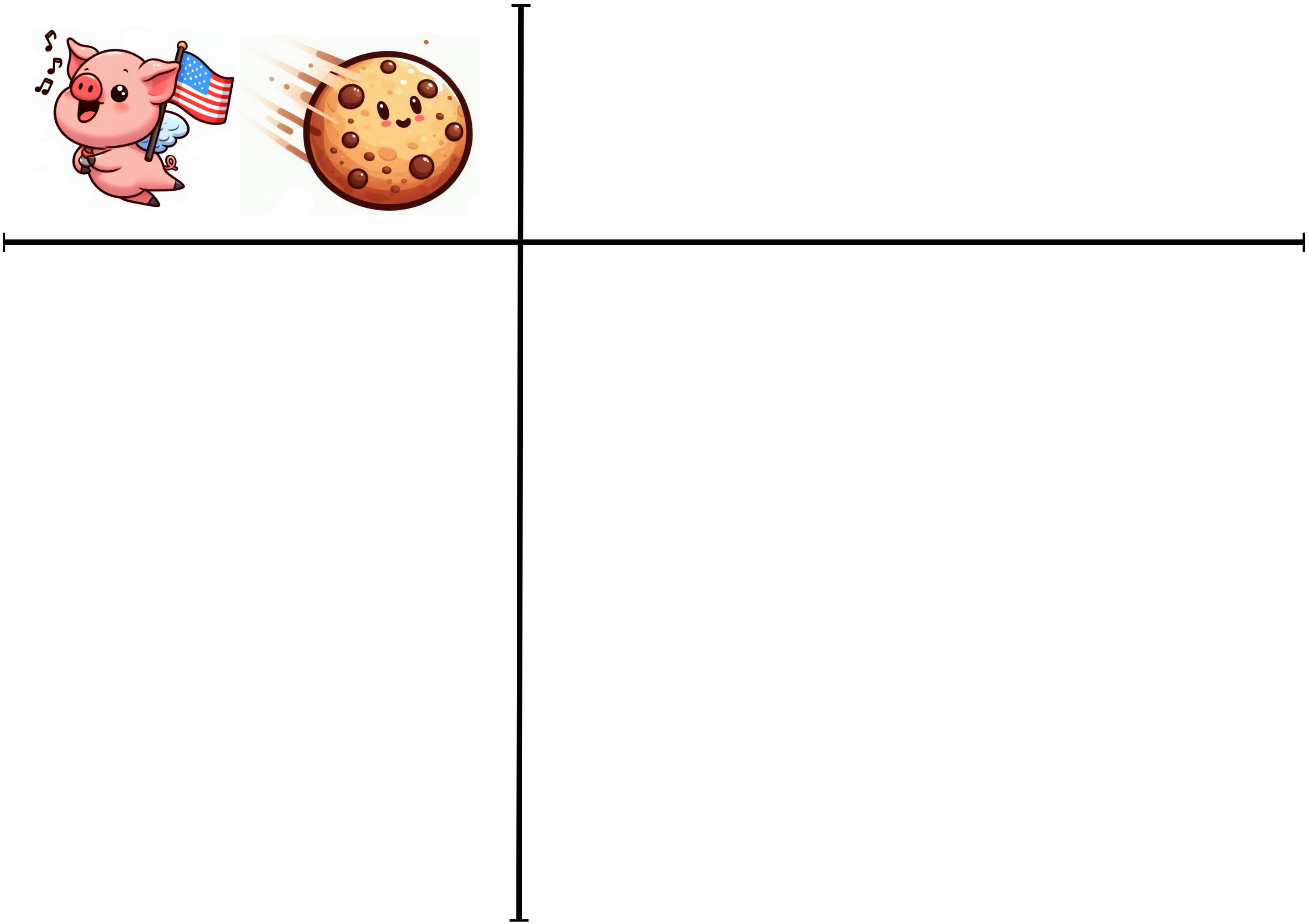
An ***implication*** is a statement of the form "If P is true, then Q is true."

If a flying pig bursts into the room and sings a pitch-perfect version of the national anthem, then Sean will throw cookies to the class.

Let's explore the definition and nature of implication through this example!

"If , then ."

An ***implication*** is a statement of the form "If P is true, then Q is true."

What is the status of our
“if , then ” contract?

What is the status of our "if , then " contract?

What is the status of our “if , then ” contract?

What is the status of our "if , then " contract?

contract is not violated

 	What is the status of our “if , then ” contract?
	contract is not violated

 	What is the status of our "if , then " contract?
	contract is not violated

 	What is the status of our “if , then ” contract?
	contract is not violated

 	What is the status of our "if , then " contract?
	contract is not violated
	contract **is** violated

 	What is the status of our “if , then ” contract?
	contract is not violated
	contract **is** violated

 	What is the status of our “if , then ” contract?
	contract is not violated
	contract **is** violated

 	What is the status of our “if , then ” contract?
	contract is not violated
	contract **is** violated

 	What is the status of our “if , then ” contract?
	contract is not violated
	contract **is** violated
	contract is not violated

 	What is the status of our “if , then ” contract?
	contract is not violated
	contract **is** violated
	contract is not violated

 	What is the status of our "if , then " contract?
	contract is not violated
	contract **is** violated
	contract is not violated

 	What is the status of our "if , then " contract?
	contract is not violated
	contract **is** violated
	contract is not violated

 	What is the status of our “if , then ” contract?
	contract is not violated
	contract **is** violated
	contract is not violated
	contract is not violated

What is the status of our “if , then ” contract?

This one often surprises people! It's part of our **definition** of implication and diverges from how conditional statements work in code.

	contract is not violated

	What is the status of our “if , then ” contract?
	contract is not violated
	contract **is** violated
	contract is not violated
	contract is not violated

What is the status of our
f , then ” contract?

This one reveals how to negate an implication!

contract is not violated

contract **is** violated

contract is not violated

contract is not violated

This one reveals how to negate an implication!

What is the status of our "if [pig], then [cookie]" contract?

contract is not violated

contract **is** violated

contract is not violated

The only time "if P, then Q" is false is when *P* is true and *Q* is false.

...olated

What Implications Mean

"If there's a rainbow in the sky, then it's raining somewhere."

- In mathematics, implication is directional.
  - The above statement doesn't mean that if it's raining somewhere, there has to be a rainbow.
- In mathematics, implications only say something about the consequent when the antecedent is true.
  - If there's no rainbow, it doesn't mean there's no rain.
- In mathematics, implication says nothing about causality.
  - Rainbows do not cause rain.

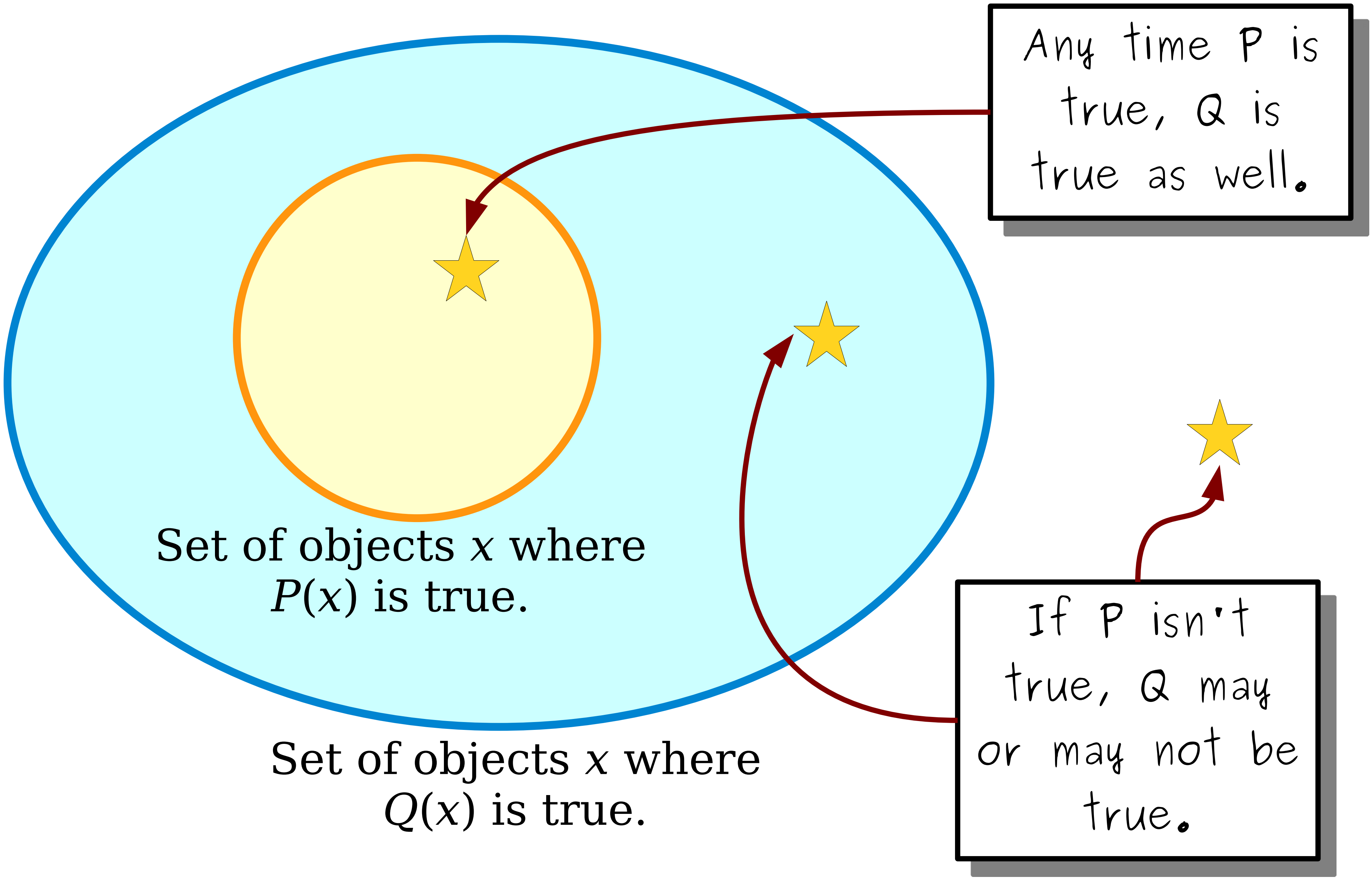
What Implications Mean

- In mathematics, a statement of the form

  For any x, if $P(x)$ is true, then $Q(x)$ is true

  means that any time you find an object x where $P(x)$ is true, you will see that $Q(x)$ is also true (for that same x).
- There is no discussion of causation here. It simply means that if you find that $P(x)$ is true, you'll find that $Q(x)$ is also true.

Implication, Diagrammatically



How do you negate an implication?

Consider once again the
"if , then "
contract.

Question: What has to happen for this contract to be broken?

Answer: A flying pig sings the national anthem, but Sean doesn't throw cookies to the class.

 	What is the status of our "if , then " contract?
	contract is not violated
	contract **is** violated
	contract is not violated
	contract is not violated

	What is the status of our “if , then ” contract?
	contract is not violated
	contract **is** violated
	contract is not violated
	contract is not violated

Key take-away!

The negation of the statement

"For any x, if $P(x)$ is true, then $Q(x)$ is true"

is the statement

"There is at least one x where $P(x)$ is true and $Q(x)$ is false."

The negation of an implication is not an implication!

Key take-away!

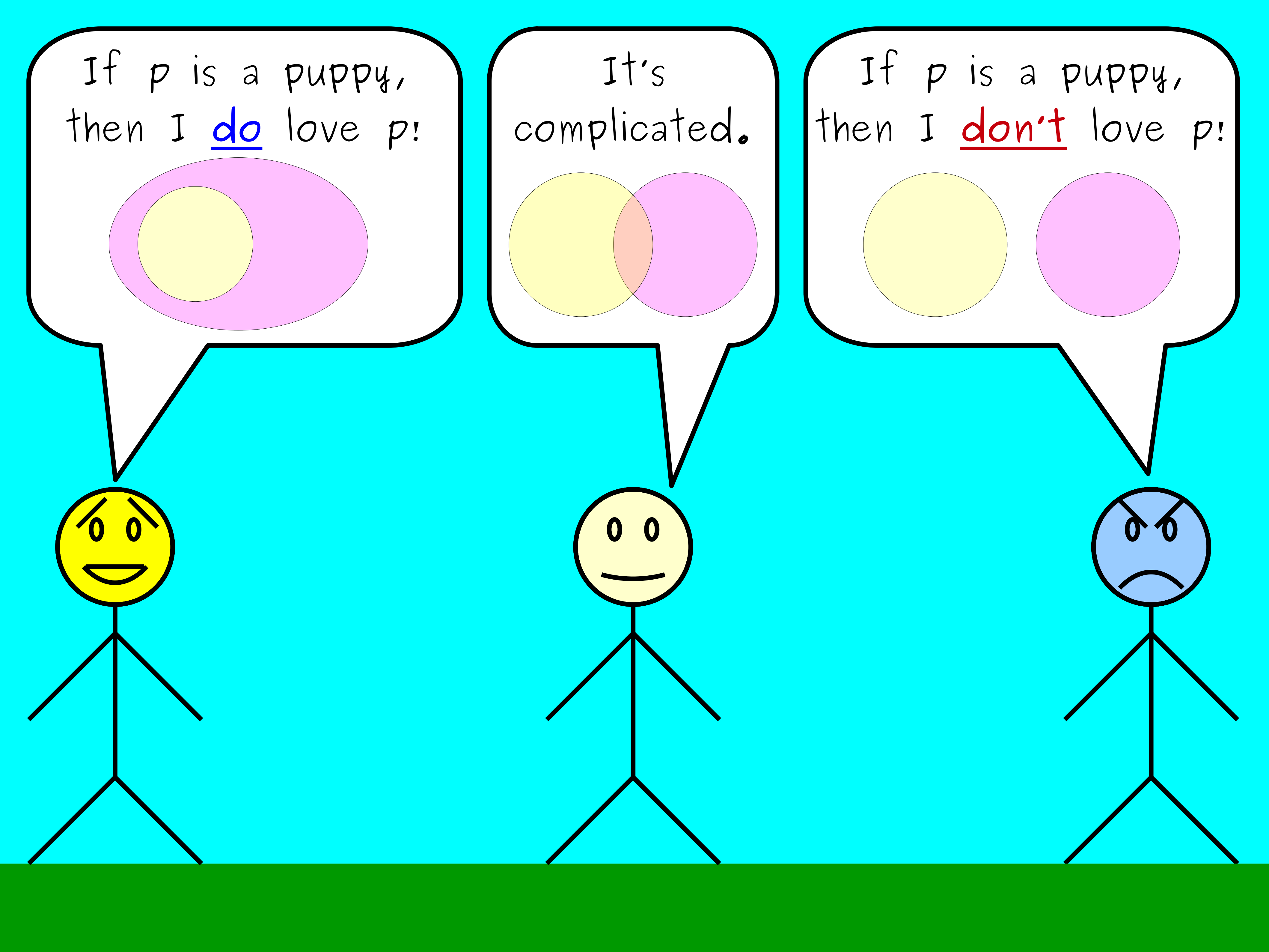
The negation of the statement

"For any *x*, if *P*(*x*) is true, then *Q*(*x*) is true"

is the statement

"There is at least one *x* where *P*(*x*) is true and *Q*(*x*) is false."

The negation of an implication is not an implication!


If p is a puppy, then I do love p!
It's complicated.
If p is a puppy, then I don't love p!

How to Negate Universal Statements:

"For all *x*, *P*(*x*) is true"

becomes

"There is an *x* where *P*(*x*) is false."

How to Negate Existential Statements:

"There exists an *x* where *P*(*x*) is true"

becomes

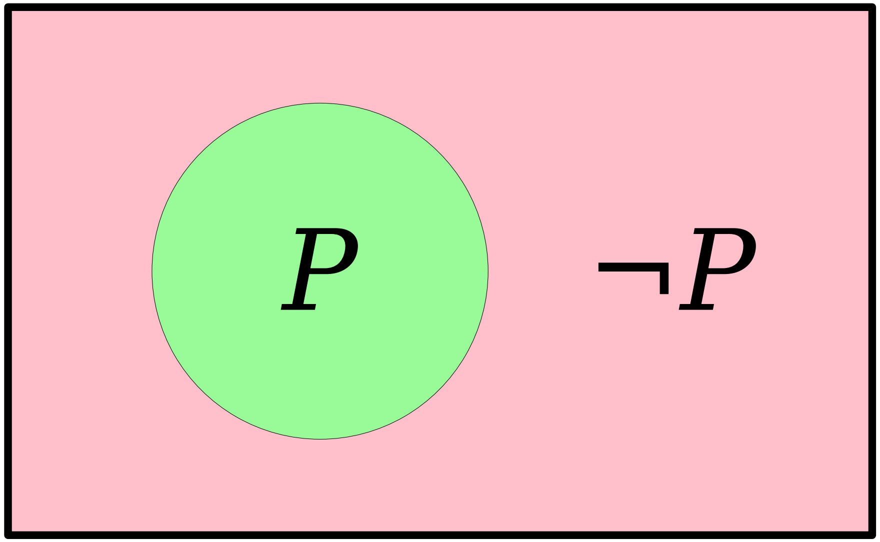
"For all *x*, *P*(*x*) is false."

How to Negate Implications:

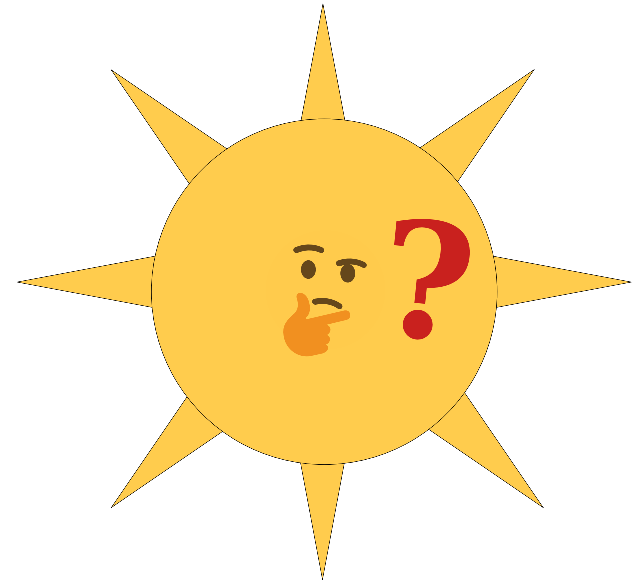
"For every *x*, if *P*(*x*) is true, then *Q*(*x*) is true"

becomes

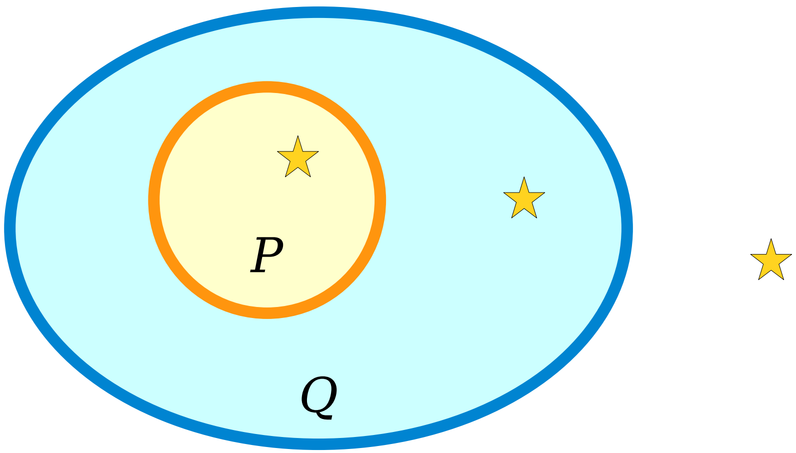
"There is an *x* where *P*(*x*) is true and *Q*(*x*) is false."



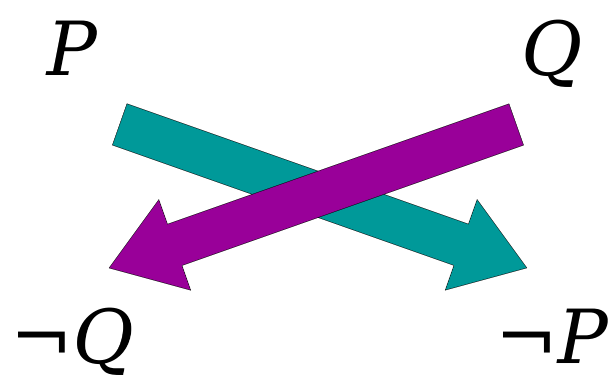
Logical Negation



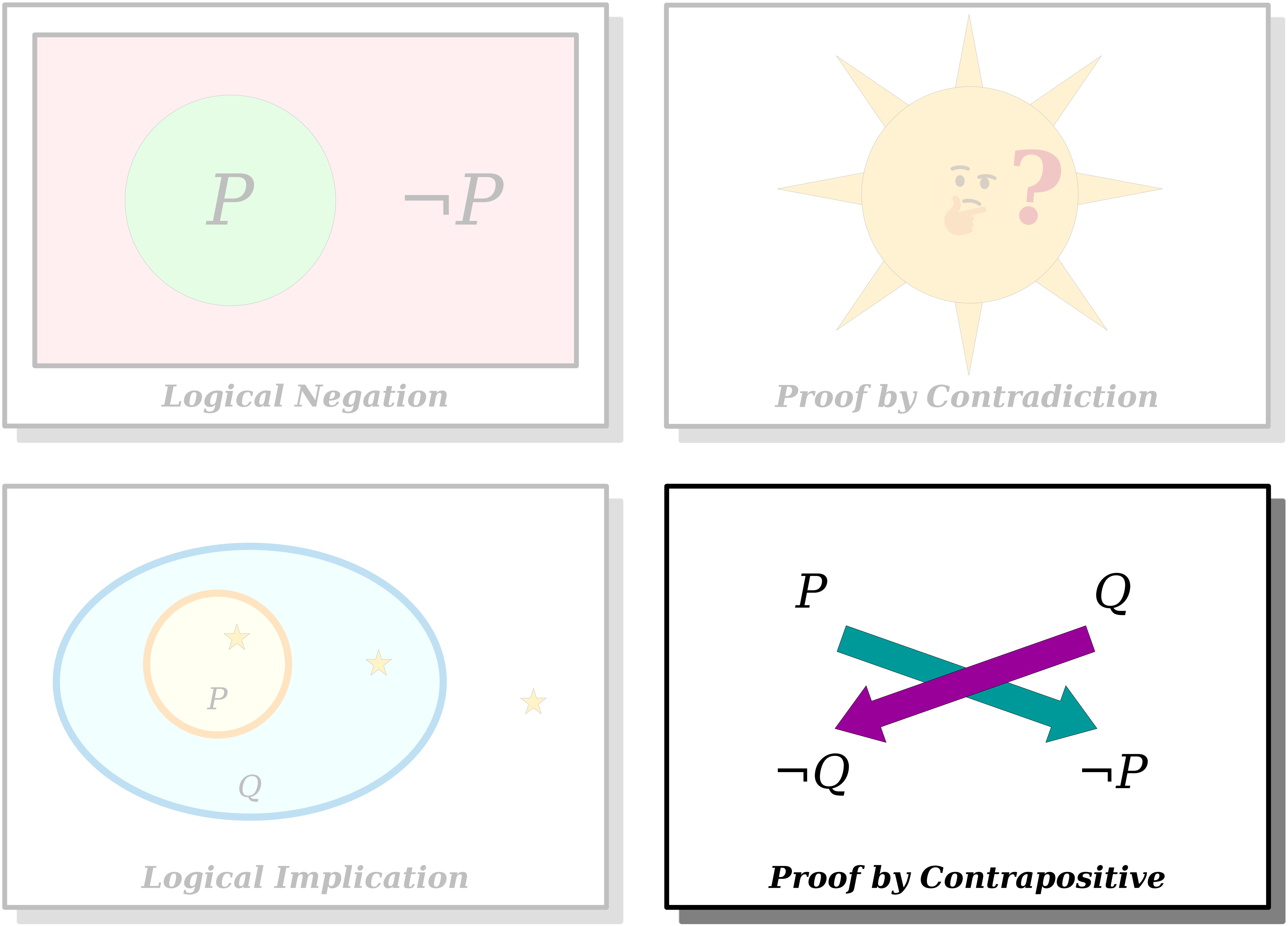
Proof by Contradiction



Logical Implication



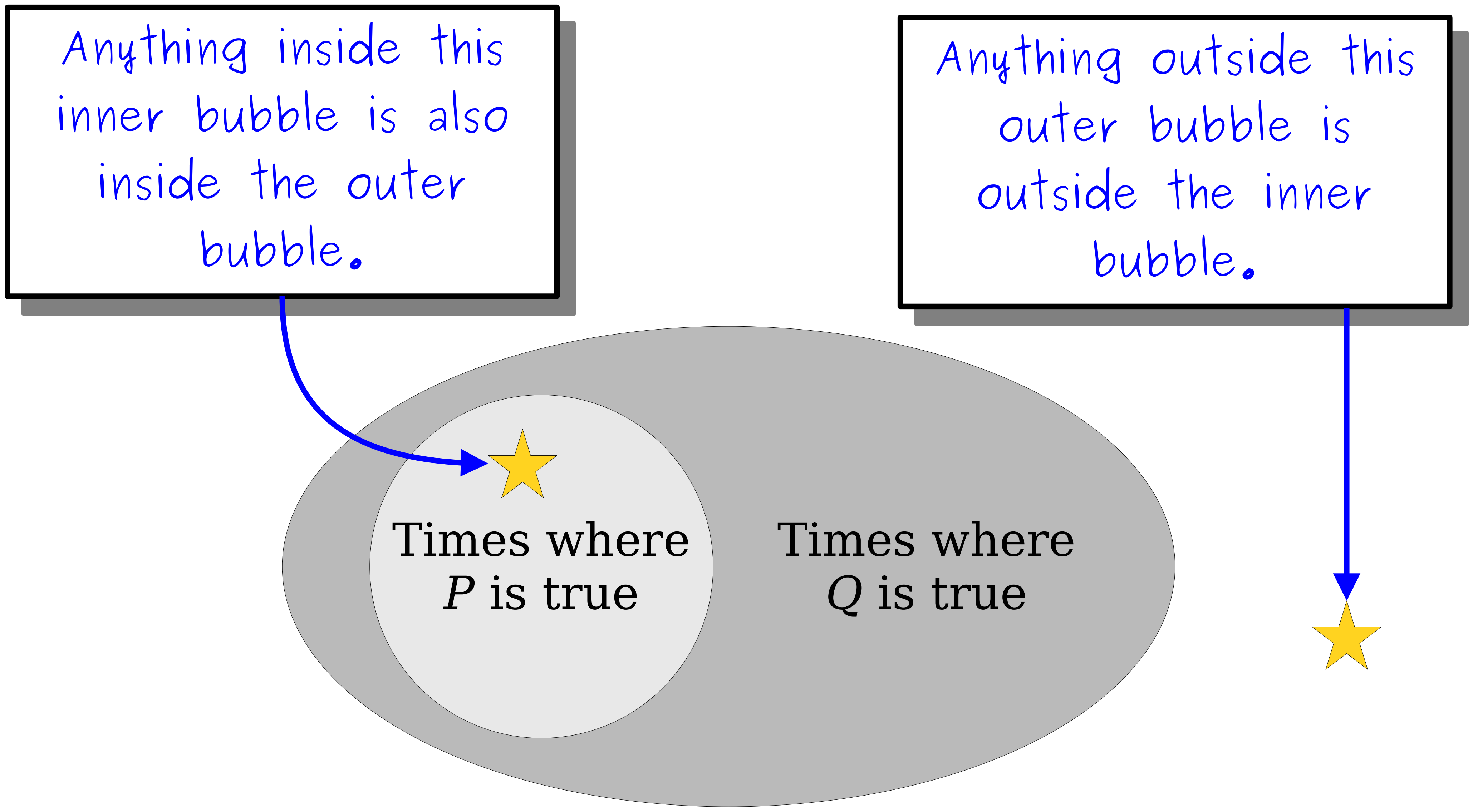
Proof by Contrapositive



P
¬P
Logical Negation
?
Proof by Contradiction
P
Q
Logical Implication
P
Q
¬Q
¬P
Proof by Contrapositive

Act IV

Proof by Contrapositive



If P is true, then Q is true.

If Q is false, then P is false.

The Contrapositive

- The ***contrapositive*** of the implication

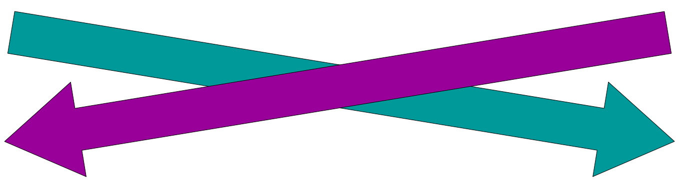
  If *P* is true, then *Q* is true

  is the implication

  If *Q* is false, then *P* is false.

- The contrapositive of an implication means exactly the same thing as the implication itself.

If it's a puppy, then I love it.



If I don't love it, then it's not a puppy.

The Contrapositive

- The ***contrapositive*** of the implication

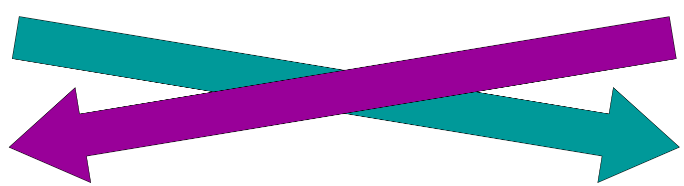
  If *P* is true, then *Q* is true

  is the implication

  If *Q* is false, then *P* is false.

- The contrapositive of an implication means exactly the same thing as the implication itself.

If I store cat food inside, then raccoons won't steal it.



If raccoons stole the cat food, then I didn't store it inside.

To prove the statement

“if *P* is true, then *Q* is true,”

you can choose to instead prove the equivalent statement

“if *Q* is false, then *P* is false,”

if that seems easier.

This is called a ***proof by contrapositive***.

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: We will prove the contrapositive of this statement.

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: We will prove the contrapositive of this statement.

This is a courtesy to the reader and says "heads up! we're not going to do a regular old-fashioned direct proof here."

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: We will prove the contrapositive of this statement.

What is the contrapositive of this statement?

if n^2 is even, then n is even.

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: We will prove the contrapositive of this statement.

What is the contrapositive of this statement?

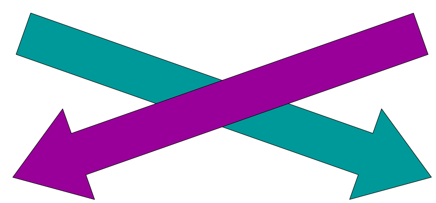
if n^2 is even, then n is even.

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: We will prove the contrapositive of this statement.

What is the contrapositive of this statement?

if n^2 is even, then n is even.

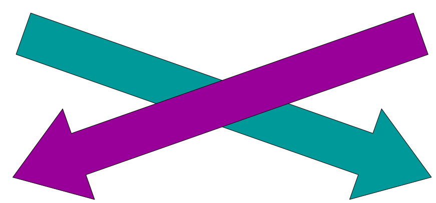


Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: We will prove the contrapositive of this statement.

What is the contrapositive of this statement?

if n^2 is even, then n is even.



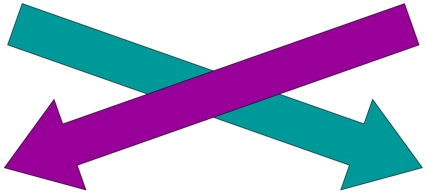
If n is odd, then n^2 is odd.

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: We will prove the contrapositive of this statement, that if n is odd, then n^2 is odd.

What is the contrapositive of this statement?

if n^2 is even, then n is even.



If n is odd, then n^2 is odd.

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: We will prove the contrapositive of this statement, that if n is odd, then n^2 is odd.

Here, we're explicitly writing out the contrapositive. This tells the reader what we're going to prove. It also acts as a sanity check by forcing us to write out what we think the contrapositive is.

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: We will prove the contrapositive of this statement, that if n is odd, then n^2 is odd.

We've said that we're going to prove this new implication, so let's go do it! The rest of this proof will look a lot like a standard direct proof.

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: We will prove the contrapositive of this statement, that if n is odd, then n^2 is odd. So let n be an arbitrary odd integer; we'll show that n^2 is odd as well.

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: We will prove the contrapositive of this statement, that if n is odd, then n^2 is odd. So let n be an arbitrary odd integer; we'll show that n^2 is odd as well.

We know that n is odd, which means there is an integer k such that $n = 2k + 1$.

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: We will prove the contrapositive of this statement, that if n is odd, then n^2 is odd. So let n be an arbitrary odd integer; we'll show that n^2 is odd as well.

We know that n is odd, which means there is an integer k such that $n = 2k + 1$. This in turn tells us that

$$n^2 = (2k + 1)^2$$

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: We will prove the contrapositive of this statement, that if n is odd, then n^2 is odd. So let n be an arbitrary odd integer; we'll show that n^2 is odd as well.

We know that n is odd, which means there is an integer k such that $n = 2k + 1$. This in turn tells us that

$$\begin{aligned} n^2 &= (2k+1)^2 \\ &= 4k^2 + 4k + 1 \end{aligned}$$

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: We will prove the contrapositive of this statement, that if n is odd, then n^2 is odd. So let n be an arbitrary odd integer; we'll show that n^2 is odd as well.

We know that n is odd, which means there is an integer k such that $n = 2k + 1$. This in turn tells us that

$$\begin{aligned} n^2 &= (2k+1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1. \end{aligned}$$

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: We will prove the contrapositive of this statement, that if n is odd, then n^2 is odd. So let n be an arbitrary odd integer; we'll show that n^2 is odd as well.

We know that n is odd, which means there is an integer k such that $n = 2k + 1$. This in turn tells us that

$$\begin{aligned} n^2 &= (2k + 1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1. \end{aligned}$$

From this, we see that there is an integer m (namely, $2k^2 + 2k$) such that $n^2 = 2m + 1$.

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: We will prove the contrapositive of this statement, that if n is odd, then n^2 is odd. So let n be an arbitrary odd integer; we'll show that n^2 is odd as well.

We know that n is odd, which means there is an integer k such that $n = 2k + 1$. This in turn tells us that

$$\begin{aligned} n^2 &= (2k+1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1. \end{aligned}$$

From this, we see that there is an integer m (namely, $2k^2 + 2k$) such that $n^2 = 2m + 1$. That means that n^2 is odd, which is what we needed to show.

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: We will prove the contrapositive of this statement, that if n is odd, then n^2 is odd. So let n be an arbitrary odd integer; we'll show that n^2 is odd as well.

We know that n is odd, which means there is an integer k such that $n = 2k + 1$. This in turn tells us that

$$\begin{aligned} n^2 &= (2k + 1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1. \end{aligned}$$

From this, we see that there is an integer m (namely, $2k^2 + 2k$) such that $n^2 = 2m + 1$. That means that n^2 is odd, which is what we needed to show. ■

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: We will prove the contrapositive of this statement, that if n is odd, then n^2 is odd. So let n be an arbitrary odd integer; we'll show that n^2 is odd

We know
integer
us that

From th
(namely
means t
to show. ■

The general pattern here is the following:

1. Start by announcing that we're going to use a proof by contrapositive so that the reader knows what to expect.

2. Explicitly state the contrapositive of what we want to prove.

3. Go prove the contrapositive.

Theorem: For any $n \in \mathbb{Z}$, if n^2 is even, then n is even.

Proof: We will prove the contrapositive of this statement, that if n is odd, then n^2 is odd. So let n be an arbitrary odd integer; we'll show that n^2 is odd as well.

We know that n is odd, which means there is an integer k such that $n = 2k + 1$. This in turn tells us that

$$\begin{aligned} n^2 &= (2k + 1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1. \end{aligned}$$

From this, we see that there is an integer m (namely, $2k^2 + 2k$) such that $n^2 = 2m + 1$. That means that n^2 is odd, which is what we needed to show. ■

Biconditionals

- The previous theorem, combined with what we saw on Wednesday, tells us the following:

  For any integer *n*, if *n* is even, then n^2 is even.

  For any integer *n*, if n^2 is even, then *n* is even.

- These are two different implications, each going the other way.
- We use the phrase ***if and only if*** to indicate that two statements imply one another.
- For example, we might combine the two above statements to say

  for any integer *n*: *n* is even if and only if n^2 is even.

Proving Biconditionals

- To prove a theorem of the form

  ***P* if and only if *Q*,**

  you need to prove two separate statements.
  - First, that if P is true, then Q is true.
  - Second, that if Q is true, then P is true.
- You can use any proof techniques you'd like to show each of these statements.
  - In our case, we used a direct proof for one and a proof by contrapositive for the other.

What We Learned

- ***How do you negate formulas?***
  - It depends on the formula. There are nice rules for how to negate universal and existential statements and implications.
- ***What's a proof by contradiction?***
  - It's a proof of a statement P that works by showing that P cannot be false.
- ***What's an implication?***
  - It's statement of the form “if P, then Q,” and states that if P is true, then Q is true.
- ***What is a proof by contrapositive?***
  - It's a proof of an implication that instead proves its contrapositive.
  - (The contrapositive of “if P, then Q” is “if not Q, then not P.”)

Your Action Items

- ***Read "Guide to Office Hours," the "Proofwriting Checklist," and the "Guide to LaTeX."***
  - There's a lot of useful information there. In particular, be sure to read the Proofwriting Checklist, as we'll be working through this checklist when grading your proofs!
- ***Start working on PS1.***
  - At a bare minimum, read over it to see what's being asked. That'll give you time to turn things over in your mind this weekend.

Next Time

- ***Mathematical Logic***
  - How do we formalize the reasoning from our proofs?
- ***Propositional Logic***
  - Reasoning about simple statements.
- ***Propositional Equivalences***
  - Simplifying complex statements.

Appendix: Proving Implications by Contradiction

Proving Implications

- Suppose we want to prove this implication:

  If *P* is true, then *Q* is true.

- We have three options available to us:
  - ***Direct Proof:***
  - ***Proof by Contrapositive.***
  - ***Proof by Contradiction.***

Proving Implications

- Suppose we want to prove this implication:

  If *P* is true, then *Q* is true.

- We have three options available to us:
  - ***Direct Proof:***

    Assume ***P* is true**, then prove ***Q* is true**.
  - ***Proof by Contrapositive.***
  - ***Proof by Contradiction.***

Proving Implications

- Suppose we want to prove this implication:

  If *P* is true, then *Q* is true.

- We have three options available to us:
  - ***Direct Proof:***

    Assume ***P* is true**, then prove ***Q* is true**.
  - ***Proof by Contrapositive.***

    Assume ***Q* is false**, then prove that ***P* is false**.
  - ***Proof by Contradiction.***

Proving Implications

- Suppose we want to prove this implication:

  If *P* is true, then *Q* is true.

- We have three options available to us:
  - ***Direct Proof:***

    Assume ***P* is true**, then prove ***Q* is true**.
  - ***Proof by Contrapositive.***

    Assume ***Q* is false**, then prove that ***P* is false**.
  - ***Proof by Contradiction.***

    … what does this look like?

Theorem: For any integer n, if n^2 is even, then n is even.

Theorem: For any integer n, if n^2 is even, then n is even.

What is the negation of our theorem?

Theorem: For any integer n, if n^2 is even, then n is even.

Proof: Assume for the sake of contradiction that there is an integer n where n^2 is even, but n is odd.

Theorem: For any integer n, if n^2 is even, then n is even.

Proof: Assume for the sake of contradiction that there is an integer n where n^2 is even, but n is odd.

Theorem: For any integer n, if n^2 is even, then n is even.

Proof: Assume for the sake of contradiction that there is an integer n where n^2 is even, but n is odd.

Since n is odd we know that there is an integer k such that

$$n = 2k + 1. \tag{1}$$

Theorem: For any integer n, if n^2 is even, then n is even.

Proof: Assume for the sake of contradiction that there is an integer n where n^2 is even, but n is odd.

Since n is odd we know that there is an integer k such that

$$n = 2k + 1. \tag{1}$$

Squaring both sides of equation (1) and simplifying gives the following:

$$n^2 = (2k + 1)^2$$

Theorem: For any integer n, if n^2 is even, then n is even.

Proof: Assume for the sake of contradiction that there is an integer n where n^2 is even, but n is odd.

Since n is odd we know that there is an integer k such that

$$n = 2k + 1. \quad (1)$$

Squaring both sides of equation (1) and simplifying gives the following:

$$\begin{aligned} n^2 &= (2k + 1)^2 \\ &= 4k^2 + 4k + 1 \end{aligned}$$

Theorem: For any integer n, if n^2 is even, then n is even.

Proof: Assume for the sake of contradiction that there is an integer n where n^2 is even, but n is odd.

Since n is odd we know that there is an integer k such that

$$n = 2k + 1. \qquad (1)$$

Squaring both sides of equation (1) and simplifying gives the following:

$$\begin{aligned} n^2 &= (2k + 1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1. \qquad (2) \end{aligned}$$

Theorem: For any integer n, if n^2 is even, then n is even.
Proof: Assume for the sake of contradiction that there is an integer n where n^2 is even, but n is odd.

Since n is odd we know that there is an integer k such that

$$n = 2k + 1. \qquad (1)$$

Squaring both sides of equation (1) and simplifying gives the following:

$$\begin{aligned} n^2 &= (2k + 1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1. \qquad (2) \end{aligned}$$

Equation (2) tells us that n^2 is odd, which is impossible; by assumption, n^2 is even.

Theorem: For any integer n, if n^2 is even, then n is even.
Proof: Assume for the sake of contradiction that there is an integer n where n^2 is even, but n is odd.

Since n is odd we know that there is an integer k such that

$$n = 2k + 1. \qquad (1)$$

Squaring both sides of equation (1) and simplifying gives the following:

$$\begin{aligned} n^2 &= (2k + 1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1. \qquad (2) \end{aligned}$$

Equation (2) tells us that n^2 is odd, which is impossible; by assumption, n^2 is even.

We have reached a contradiction, so our assumption must have been incorrect.

Theorem: For any integer n, if n^2 is even, then n is even.
Proof: Assume for the sake of contradiction that there is an integer n where n^2 is even, but n is odd.

Since n is odd we know that there is an integer k such that

$$n = 2k + 1. \tag{1}$$

Squaring both sides of equation (1) and simplifying gives the following:

$$\begin{aligned} n^2 &= (2k + 1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1. \qquad (2) \end{aligned}$$

Equation (2) tells us that n^2 is odd, which is impossible; by assumption, n^2 is even.

We have reached a contradiction, so our assumption must have been incorrect. Thus if n is an integer and n^2 is even, n is even as well.

Theorem: For any integer n, if n^2 is even, then n is even.
Proof: Assume for the sake of contradiction that there is an integer n where n^2 is even, but n is odd.

Since n is odd we know that there is an integer k such that

$$n = 2k + 1. \tag{1}$$

Squaring both sides of equation (1) and simplifying gives the following:

$$\begin{aligned} n^2 &= (2k+1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1. \end{aligned} \tag{2}$$

Equation (2) tells us that n^2 is odd, which is impossible; by assumption, n^2 is even.

We have reached a contradiction, so our assumption must have been incorrect. Thus if n is an integer and n^2 is even, n is even as well. ■

Theorem: For any integer n, if n^2 is even, then n is even.
Proof: Assume for the sake of contradiction that there is an integer n where n^2 is even, but n is odd.

Since n is odd we know that there is an integer k such

The three key pieces:

1. Say that the proof is by contradiction.
2. Say what the negation of the original statement is.
3. Say you have reached a contradiction and what the contradiction entails.

In CS103, please include all these steps in your proofs!

Equation (2) tells us that n^2 is odd, which is impossible; by assumption, n^2 is even.

We have reached a contradiction, so our assumption must have been incorrect. Thus if n is an integer and n^2 is even, n is even as well. ■

Theorem: For any integer n, if n^2 is even, then n is even.

Proof: Assume for the sake of contradiction that there is an integer n where n^2 is even, but n is odd.

Since n is odd we know that there is an integer k such that

$$n = 2k + 1. \qquad (1)$$

Squaring both sides of equation (1) and simplifying gives the following:

$$\begin{aligned} n^2 &= (2k + 1)^2 \\ &= 4k^2 + 4k + 1 \\ &= 2(2k^2 + 2k) + 1. \qquad (2) \end{aligned}$$

Equation (2) tells us that n^2 is odd, which is impossible; by assumption, n^2 is even.

We have reached a contradiction, so our assumption must have been incorrect. Thus if n is an integer and n^2 is even, n is even as well. ■

Proving Implications

- Suppose we want to prove this implication:

  If *P* is true, then *Q* is true.

- We have three options available to us:
  - ***Direct Proof:***

    Assume ***P*** **is true**, then prove ***Q*** **is true**.
  - ***Proof by Contrapositive.***

    Assume ***Q*** **is false**, then prove that ***P*** **is false**.
  - ***Proof by Contradiction.***

    Assume ***P is true*** and ***Q is false***, then derive a contradiction.