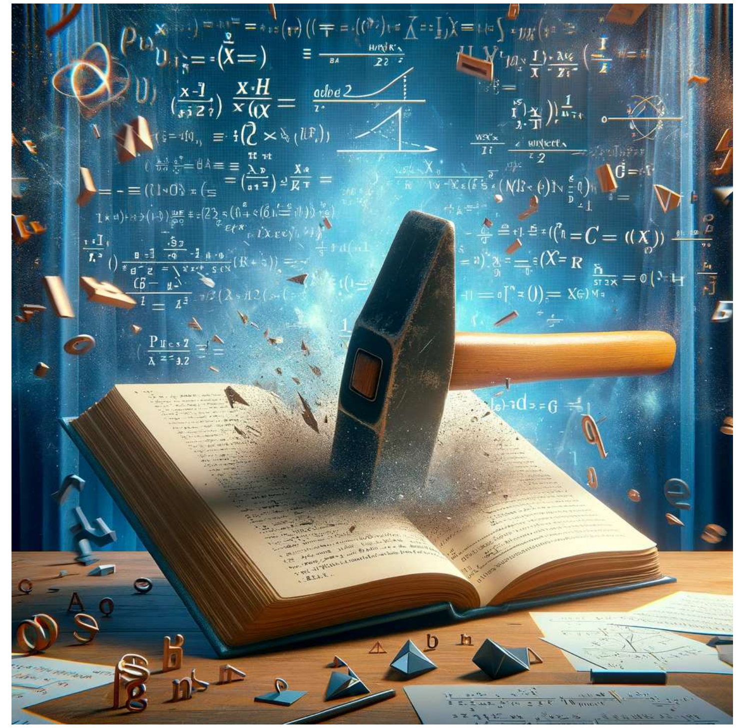


Proof By Contradiction

In real life!

- Claim: My Tire is Leaking
- Suppose that this tire was not leaking
- This means the tire pressure should be constant
- I observe the pressure is dropping at a moderate rate
- But there should be constant pressure if it was not leaking
- Therefore, it must be leaking

Proof by Contradiction Skeleton

Claim: p is true.

- Suppose for the sake of contradiction $\neg p$.
- …
- Then some statement s must hold.
- …
- And some statement $\neg s$ must hold.
- But s and $\neg s$ is a contradiction. So p must be true.

My tire is leaking

Suppose my tire is not leaking

The tire pressure must be constant

The tire pressure is decreasing

My Tire is leaking

Why does this work?

Let's say the claim you are trying to prove is p.

A proof by contradiction shows the following implication:

$$\neg p \rightarrow False$$

Why does this implication show p?

Hint think contrapositive

The contrapositive is $True \rightarrow p$ which simplifies to just p.

This means that by proving $\neg p \rightarrow False$, you have proved p is True!

Proof By Contradiction

If a^2 is even, then a is even

Claim: $\sqrt{2}$ is irrational (i.e not rational)

Proof:

Proof By Contradiction

If a^2 is even, then a is even

Claim: $\sqrt{2}$ is irrational (i.e not rational)

Proof:

Suppose for the sake of contradiction that $\sqrt{2}$ is rational

Notice target is unknown

But [] is a contradiction! Thus, we can conclude that $\sqrt{2}$ is irrational.

Proof By Contradiction

If a^2 is even, then a is even

Claim: $\sqrt{2}$ is irrational (i.e not rational)

Proof:

Suppose for the sake of contradiction that $\sqrt{2}$ is rational.

By definition of rational, there are integers s, t such that $t \neq 0$ and $\sqrt{2} = \frac{s}{t}$

Without loss of generality, suppose that s, t are in lowest terms (i.e it is the reduced fraction and 1 is s, t greatest common factor)

But [] is a contradiction! Thus, we can conclude that $\sqrt{2}$ is irrational.

What is "Without Loss of Generality"?

You can use this when it looks like you are introducing a new assumption, but you are not, and the claim is still general. Only use if it would be immediately obvious to the reader why it is the case

In this case: if s and t share a factor other than 1, i.e k, we can just cancel out their common factor and continue the proof. (i.e $\frac{s\prime k}{t\prime k} = \frac{s}{t}$)

Another example:

Let x,y be integers; without loss of generality, assume $x \geq y$.

Proof By Contradiction

If a^2 is even, then a is even

Claim: $\sqrt{2}$ is irrational (i.e not rational)

Proof:

Suppose for the sake of contradiction that $\sqrt{2}$ is rational.

By definition of rational, there are integers s, t such that $t \neq 0$ and $\sqrt{2} = \frac{s}{t}$

Without loss of generality, suppose that s, t are in lowest terms (i.e it is the reduced fraction and 1 is s, t greatest common factor)

But [] is a contradiction! Thus, we can conclude that $\sqrt{2}$ is irrational.

Proof By Contradiction

If a^2 is even, then a is even

Claim: $\sqrt{2}$ is irrational (i.e not rational)

Proof:

Suppose for the sake of contradiction that $\sqrt{2}$ is rational.

By definition of rational, there are integers s, t such that $t \neq 0$ and $\sqrt{2} = \frac{s}{t}$

Without loss of generality, suppose that s, t are in lowest terms (i.e it is the reduced fraction and 1 is s, t greatest common factor)

$\sqrt{2} = \frac{s}{t}$

But [] is a contradiction! Thus, we can conclude that $\sqrt{2}$ is irrational.

Proof By Contradiction

If a^2 is even, then a is even

Claim: $\sqrt{2}$ is irrational (i.e not rational)

Proof:

Suppose for the sake of contradiction that $\sqrt{2}$ is rational.

By definition of rational, there are integers s, t such that $t \neq 0$ and $\sqrt{2} = \frac{s}{t}$

Without loss of generality, suppose that s, t are in lowest terms (i.e it is the reduced fraction and 1 is s, t greatest common factor)

$\sqrt{2} = \frac{s}{t}$

$2 = \frac{s^2}{t^2}$

But [] is a contradiction! Thus, we can conclude that $\sqrt{2}$ is irrational.

Proof By Contradiction

If a^2 is even, then a is even

Claim: $\sqrt{2}$ is irrational (i.e not rational)

Proof:

Suppose for the sake of contradiction that $\sqrt{2}$ is rational.

By definition of rational, there are integers s, t such that $t \neq 0$ and $\sqrt{2} = \frac{s}{t}$

Without loss of generality, suppose that s, t are in lowest terms (i.e it is the reduced fraction and 1 is s, t greatest common factor)

$\sqrt{2} = \frac{s}{t}$

$2 = \frac{s^2}{t^2}$

Thus: $2t^2 = s^2$

But [] is a contradiction! Thus, we can conclude that $\sqrt{2}$ is irrational.

Proof By Contradiction

If a^2 is even, then a is even

Claim: $\sqrt{2}$ is irrational (i.e not rational)

Proof:

Suppose for the sake of contradiction that $\sqrt{2}$ is rational.

By definition of rational, there are integers s, t such that $t \neq 0$ and $\sqrt{2} = \frac{s}{t}$

Without loss of generality, suppose that s, t are in lowest terms (i.e it is the reduced fraction and 1 is s, t greatest common factor)

$\sqrt{2} = \frac{s}{t}$

$2 = \frac{s^2}{t^2}$

Thus: $2t^2 = s^2$ So s^2 is even, making s even by our lemma. This means that $s = 2k$ for some integer k

But [] is a contradiction! Thus, we can conclude that $\sqrt{2}$ is irrational.

Proof By Contradiction

If a^2 is even, then a is even

Claim: $\sqrt{2}$ is irrational (i.e not rational)

Proof:

Suppose for the sake of contradiction that $\sqrt{2}$ is rational.

By definition of rational, there are integers s, t such that $t \neq 0$ and $\sqrt{2} = \frac{s}{t}$

Without loss of generality, suppose that s, t are in lowest terms (i.e it is the reduced fraction and 1 is s, t greatest common factor)

$\sqrt{2} = \frac{s}{t}$

$2 = \frac{s^2}{t^2}$

Thus: $2t^2 = s^2$ So s^2 is even, making s even by our lemma. This means that $s = 2k$ for some integer k

Squaring both sides, we get $s^2 = 4k^2$

But [] is a contradiction! Thus, we can conclude that $\sqrt{2}$ is irrational.

Proof By Contradiction

If a^2 is even, then a is even

Claim: $\sqrt{2}$ is irrational (i.e not rational)

Proof:

Suppose for the sake of contradiction that $\sqrt{2}$ is rational.

By definition of rational, there are integers s, t such that $t \neq 0$ and $\sqrt{2} = \frac{s}{t}$

Without loss of generality, suppose that s, t are in lowest terms (i.e it is the reduced fraction and 1 is s, t greatest common factor)

$\sqrt{2} = \frac{s}{t}$

$2 = \frac{s^2}{t^2}$

Thus: $2t^2 = s^2$ So s^2 is even, making s even by our lemma. This means that $s = 2k$ for some integer k

Squaring both sides, we get $s^2 = 4k^2$, which we can plug back into $2t^2 = s^2$ to get $2\text{t}^2 = 4k^2$

But [] is a contradiction! Thus, we can conclude that $\sqrt{2}$ is irrational.

Proof By Contradiction

If a^2 is even, then a is even

Claim: $\sqrt{2}$ is irrational (i.e not rational)

Proof:

Suppose for the sake of contradiction that $\sqrt{2}$ is rational.

By definition of rational, there are integers s, t such that $t \neq 0$ and $\sqrt{2} = \frac{s}{t}$

Without loss of generality, suppose that s, t are in lowest terms (i.e it is the reduced fraction and 1 is s, t greatest common factor)

$\sqrt{2} = \frac{s}{t}$

$2 = \frac{s^2}{t^2}$

Thus: $2t^2 = s^2$ So s^2 is even, making s even by our lemma. This means that $s = 2k$ for some integer k

Squaring both sides, we get $s^2 = 4k^2$, which we can plug back into $2t^2 = s^2$ to get $2t^2 = 4k^2$

Dividing both sides by two, we get $t^2 = 2k^2$

But [] is a contradiction! Thus, we can conclude that $\sqrt{2}$ is irrational.

Proof By Contradiction

If a^2 is even, then a is even

Claim: $\sqrt{2}$ is irrational (i.e not rational)

Proof:

Suppose for the sake of contradiction that $\sqrt{2}$ is rational.

By definition of rational, there are integers s, t such that $t \neq 0$ and $\sqrt{2} = \frac{s}{t}$

Without loss of generality, suppose that s, t are in lowest terms (i.e it is the reduced fraction and 1 is s, t greatest common factor)

$\sqrt{2} = \frac{s}{t}$

$2 = \frac{s^2}{t^2}$

Thus: $2t^2 = s^2$ So s^2 is even, making s even by our lemma. This means that $s = 2k$ for some integer k

Squaring both sides, we get $s^2 = 4k^2$, which we can plug back into $2t^2 = s^2$ to get $2\text{t}^2 = 4k^2$

Dividing both sides by two, we get $\text{t}^2 = 2k^2$, making t^2 is even, making t even by our lemma.

But [] is a contradiction! Thus, we can conclude that $\sqrt{2}$ is irrational.

Proof By Contradiction

If a^2 is even, then a is even

Claim: $\sqrt{2}$ is irrational (i.e not rational)

Proof:

Suppose for the sake of contradiction that $\sqrt{2}$ is rational.

By definition of rational, there are integers s, t such that $t \neq 0$ and $\sqrt{2} = \frac{s}{t}$

Without loss of generality, suppose that s, t are in lowest terms (i.e it is the reduced fraction and 1 is s, t greatest common factor)

$\sqrt{2} = \frac{s}{t}$

$2 = \frac{s^2}{t^2}$

Thus: $2t^2 = s^2$ So s^2 is even, making s even by our lemma. This means that $s = 2k$ for some integer k

Squaring both sides, we get $s^2 = 4k^2$, which we can plug back into $2t^2 = s^2$ to get $2t^2 = 4k^2$

Dividing both sides by two, we get $t^2 = 2k^2$, making t^2 is even, making t even by our lemma.

But if both s and t are even, they must have a common factor of 2. But we said that the fraction $\frac{s}{t}$ was irreducible.

This is a contradiction! Thus, we can conclude that $\sqrt{2}$ is irrational.

Proof by Contradiction

Proof by contradiction is a strategy for proving statements of any form.

- The general strategy to prove p is to assume $\neg p$ and derive False.

Examples:

- The strategy to prove $p \rightarrow q$ is to assume $p \land \neg q$ and derive False.
- The strategy to prove $p \lor q$ is to assume $\neg p \land \neg q$ and derive False.
- The strategy to prove $\forall x(P(x))$ is to assume $\exists x\left(\neg P(x)\right)$ and derive False.
- The strategy to prove $\exists x(P(x))$ is to assume $\forall x(\neg P(x))$ and derive False.

Another Proof by Contradiction

Claim: There are infinitely many primes

Proof:

Another Proof by Contradiction

Claim: There are infinitely many primes

Proof:

Suppose for the sake of contradiction, there are only finitely many primes. Call them $p_1, p_2, \dots, p_k$.

But [] is a contradiction! So, there must be infinitely many primes.

Another Proof by Contradiction

Claim: There are infinitely many primes

Proof:

Suppose for the sake of contradiction, there are only finitely many primes. Call them $p_1, p_2, \dots, p_k$.

Where can we find a contradiction?

- Show our list is non inclusive (i.e create a different prime number)
- Show one of the numbers in our list is not prime
- Create a contradiction with facts about prime factorization
- Show 1 = 2
- Show p is odd and even at the same time
- Proof by cases with a mix of the above

But [] is a contradiction! So, there must be infinitely many primes.

Proof by Contradiction: Remarks

- Unlike other proof techniques, we don't know *where* we're going.
  We're trying to find any contradiction. That can make it harder.
- Contradiction is a sledge-hammer.
  It can be used to prove many things. But it makes a mess.
- You can find a contradiction directly with your assumption

Another Proof by Contradiction

Claim: There are infinitely many primes

Proof:

Suppose for the sake of contradiction, there are only finitely many primes. Call them $p_1, p_2, \ldots, p_k$.

Consider the number $q = p_1 \cdot p_2 \cdot \ldots \cdot p_k + 1$

But [] is a contradiction! So, there must be infinitely many primes.

Another Proof by Contradiction

Claim: There are infinitely many primes

Proof:

Suppose for the sake of contradiction, there are only finitely many primes. Call them $p_1, p_2, \ldots, p_k$.

Consider the number $\mathrm{q} = p_1 \cdot p_2 \cdot \ldots \cdot p_k + 1$

Case 1: q is prime:

But [] is a contradiction! So, there must be infinitely many primes.

Another Proof by Contradiction

Claim: There are infinitely many primes

Proof:

Suppose for the sake of contradiction, there are only finitely many primes. Call them $p_1, p_2, \ldots, p_k$.

Consider the number $\mathrm{q} = p_1 \cdot p_2 \cdot \ldots \cdot p_k + 1$

Case 1: q is prime:

> Notice that q is prime and must be larger that every prime in $p_1, p_2, \ldots, p_k$. But every prime was in the list, therefore this is a contradiction!

But [] is a contradiction! So, there must be infinitely many primes.

Another Proof by Contradiction

Claim: There are infinitely many primes

Proof:

Suppose for the sake of contradiction, there are only finitely many primes. Call them $p_1, p_2, \dots, p_k$.

Consider the number $\mathrm{q} = p_1 \cdot p_2 \cdot \dots \cdot p_k + 1$

Case 1: q is prime:

> Notice that q is prime and must be larger that every prime in $p_1, p_2, \dots, p_k$. But every prime was in the list, therefore this is a contradiction!

Case 2: q is not prime (i.e composite):

But [] is a contradiction! So, there must be infinitely many primes.

Another Proof by Contradiction

Claim: There are infinitely many primes

Proof:

Suppose for the sake of contradiction, there are only finitely many primes. Call them $p_1, p_2, \ldots, p_k$.

Consider the number $\mathrm{q} = p_1 \cdot p_2 \cdot \ldots \cdot p_k + 1$

Case 1: q is prime:

Notice that q is prime and must be larger that every prime in $p_1, p_2, \ldots, p_k$. But every prime was in the list, therefore this is a contradiction!

Case 2: q is not prime (i.e composite):

Since q is composite, we know that some prime p_i must divide q.

But [] is a contradiction! So, there must be infinitely many primes.

Another Proof by Contradiction

Claim: There are infinitely many primes

Proof:

Suppose for the sake of contradiction, there are only finitely many primes. Call them $p_1, p_2, \ldots, p_k$.

Consider the number $\mathrm{q} = p_1 \cdot p_2 \cdot \ldots \cdot p_k + 1$

Case 1: q is prime:

> Notice that q is prime and must be larger that every prime in $p_1, p_2, \ldots, p_k$. But every prime was in the list, therefore this is a contradiction!

Case 2: q is not prime (i.e composite):

> Since q is composite, we know that some prime p_i must divide q. This means that $q \% p_i = 0$.

But [] is a contradiction! So, there must be infinitely many primes.

Another Proof by Contradiction

Claim: There are infinitely many primes

Proof:

Suppose for the sake of contradiction, there are only finitely many primes. Call them $p_1, p_2, \ldots, p_k$.

Consider the number $\mathrm{q} = p_1 \cdot p_2 \cdot \ldots \cdot p_k + 1$

Case 1: q is prime:

Notice that q is prime and must be larger that every prime in $p_1, p_2, \ldots, p_k$. But every prime was in the list, therefore this is a contradiction!

Case 2: q is not prime (i.e composite):

Since q is composite, we know that some prime p_i must divide q. This means that $q \% p_i = 0$.

Also, notice that $\mathrm{q} \% p_i = (p_1 \cdot p_2 \cdot \ldots \cdot p_k) + 1 \ \% p_i$ using the definition of q,

But [] is a contradiction! So, there must be infinitely many primes.

Another Proof by Contradiction

Claim: There are infinitely many primes

Proof:

Suppose for the sake of contradiction, there are only finitely many primes. Call them $p_1, p_2, \dots, p_k$.

Consider the number $\mathrm{q} = p_1 \cdot p_2 \cdot \dots \cdot p_k + 1$

Case 1: q is prime:

Notice that q is prime and must be larger that every prime in $p_1, p_2, \dots, p_k$. But every prime was in the list, therefore this is a contradiction!

Case 2: q is not prime (i.e composite):

Since q is composite, we know that some prime p_i must divide q. This means that $q \;\%\; p_i = 0$.

Also, notice that $\mathrm{q} \;\%\; p_i = (p_1 \cdot p_2 \cdot \dots \cdot p_k) + 1 \;\; \%\; p_i$ using the definition of q, which gives us:

$$\mathrm{q} \;\%\; p_i =$$

But [] is a contradiction! So, there must be infinitely many primes.

Another Proof by Contradiction

Claim: There are infinitely many primes

Proof:

Suppose for the sake of contradiction, there are only finitely many primes. Call them $p_1, p_2, \ldots, p_k$.

Consider the number $\mathrm{q} = p_1 \cdot p_2 \cdot \ldots \cdot p_k + 1$

Case 1: q is prime:

> Notice that q is prime and must be larger that every prime in $p_1, p_2, \ldots, p_k$. But every prime was in the list, therefore this is a contradiction!

Case 2: q is not prime (i.e composite):

> Since q is composite, we know that some prime p_i must divide q. This means that $q \,\%\, p_i = 0$.
>
> Also, notice that $\mathrm{q} \,\%\, p_i = (p_1 \cdot p_2 \cdot \ldots \cdot p_k) + 1 \;\%\, p_i$ using the definition of q, which gives us:
>
> $$\mathrm{q} \,\%\, p_i = (p_1 \cdot p_2 \cdot \ldots \cdot p_k) + 1 \,\%\, p_i =$$

But [] is a contradiction! So, there must be infinitely many primes.

Another Proof by Contradiction

Claim: There are infinitely many primes

Proof:

Suppose for the sake of contradiction, there are only finitely many primes. Call them $p_1, p_2, \ldots, p_k$.

Consider the number $\mathrm{q} = p_1 \cdot p_2 \cdot \ldots \cdot p_k + 1$

Case 1: q is prime:

> Notice that q is prime and must be larger that every prime in $p_1, p_2, \ldots, p_k$. But every prime was in the list, therefore this is a contradiction!

Case 2: q is not prime (i.e composite):

> Since q is composite, we know that some prime p_i must divide q. This means that $q \,\%\, p_i = 0$.
>
> Also, notice that $\mathrm{q} \,\%\, p_i = (p_1 \cdot p_2 \cdot \ldots \cdot p_k) + 1 \;\%\, p_i$ using the definition of q, which gives us:
>
> $$\mathrm{q} \,\%\, p_i = (p_1 \cdot p_2 \cdot \ldots \cdot p_k) + 1 \,\%\, p_i = (p_1 \cdot \ldots p_i \cdot \ldots \cdot p_k) + 1 \,\%\, p_i$$

But [] is a contradiction! So, there must be infinitely many primes.

Another Proof by Contradiction

Claim: There are infinitely many primes

Proof:

Suppose for the sake of contradiction, there are only finitely many primes. Call them $p_1, p_2, \dots, p_k$.

Consider the number $\mathrm{q} = p_1 \cdot p_2 \cdot \dots \cdot p_k + 1$

Case 1: q is prime:

Notice that q is prime and must be larger that every prime in $p_1, p_2, \dots, p_k$. But every prime was in the list, therefore this is a contradiction!

Case 2: q is not prime (i.e composite):

Since q is composite, we know that some prime p_i must divide q. This means that $q \,\%\, p_i = 0$.

Also, notice that $\mathrm{q} \,\%\, p_i = (p_1 \cdot p_2 \cdot \dots \cdot p_k) + 1 \;\%\, p_i$ using the definition of q, which gives us:

$$\mathrm{q} \,\%\, p_i = (p_1 \cdot p_2 \cdot \dots \cdot p_k) + 1 \,\%\, p_i = (p_1 \cdot \dots p_i \cdot \dots \cdot p_k) + 1 \,\%\, p_i = 1$$

But [] is a contradiction! So, there must be infinitely many primes.

Another Proof by Contradiction

Claim: There are infinitely many primes

Proof:

Suppose for the sake of contradiction, there are only finitely many primes. Call them $p_1, p_2, \dots, p_k$.

Consider the number $\mathrm{q} = p_1 \cdot p_2 \cdot \dots \cdot p_k + 1$

Case 1: q is prime:

Notice that q is prime and must be larger that every prime in $p_1, p_2, \dots, p_k$. But every prime was in the list, therefore this is a contradiction!

Case 2: q is not prime (i.e composite):

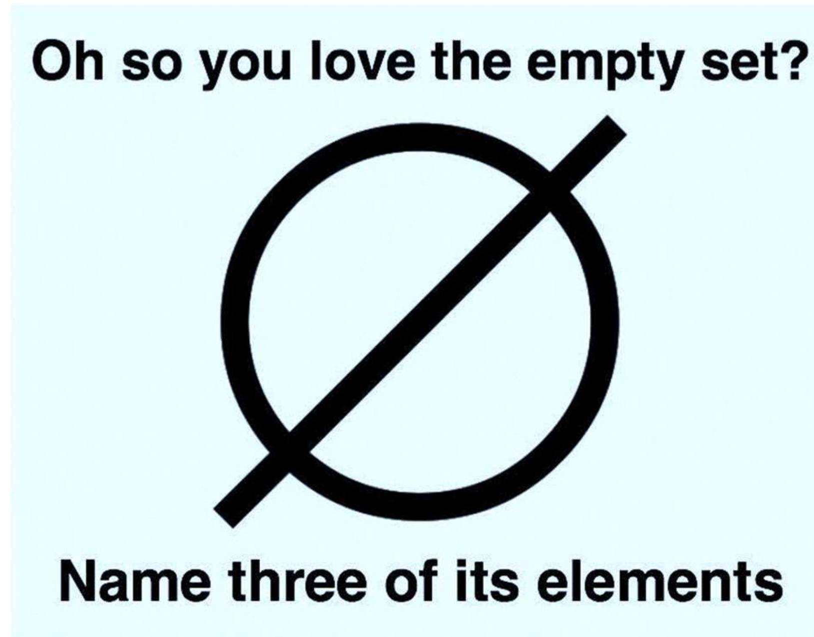
Since q is composite, we know that some prime p_i must divide q. This means that $q \,\%\, p_i = 0$.

Also, notice that $\mathrm{q} \,\%\, p_i = (p_1 \cdot p_2 \cdot \dots \cdot p_k) + 1 \;\%\, p_i$ using the definition of q, which gives us:

$$\mathrm{q} \,\%\, p_i = (p_1 \cdot p_2 \cdot \dots \cdot p_k) + 1 \,\%\, p_i = (p_1 \cdot \dots p_i \cdot \dots \cdot p_k) + 1 \,\%\, p_i = 1$$

This means that $q \,\%\, p_i$ equals both 1 and 0, which is impossible!

In both cases, this is a contradiction! So, there must be infinitely many primes.



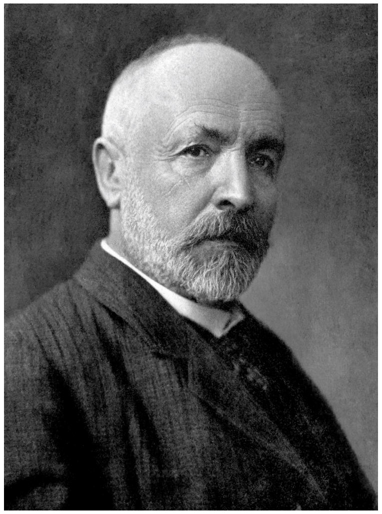
Set Theory

CSE 311: Foundations of Computing I
Lecture 10

Motivation

- Set theory is widely regarded as the foundation for all of mathematics.

- In computing, there are applications in:
- Data Structures
- Databases
- Programming Languages



Father of Modern
Set Theory
Georg Cantor
(1845 – 1918)

Sets

- Definition:
- A set is an unordered collection of distinct objects, called elements.

- We write $x \in A$ to say that x is an element of the set A.

- We write $x \notin A$ to say that x is not an element of the set A.

Set Notation

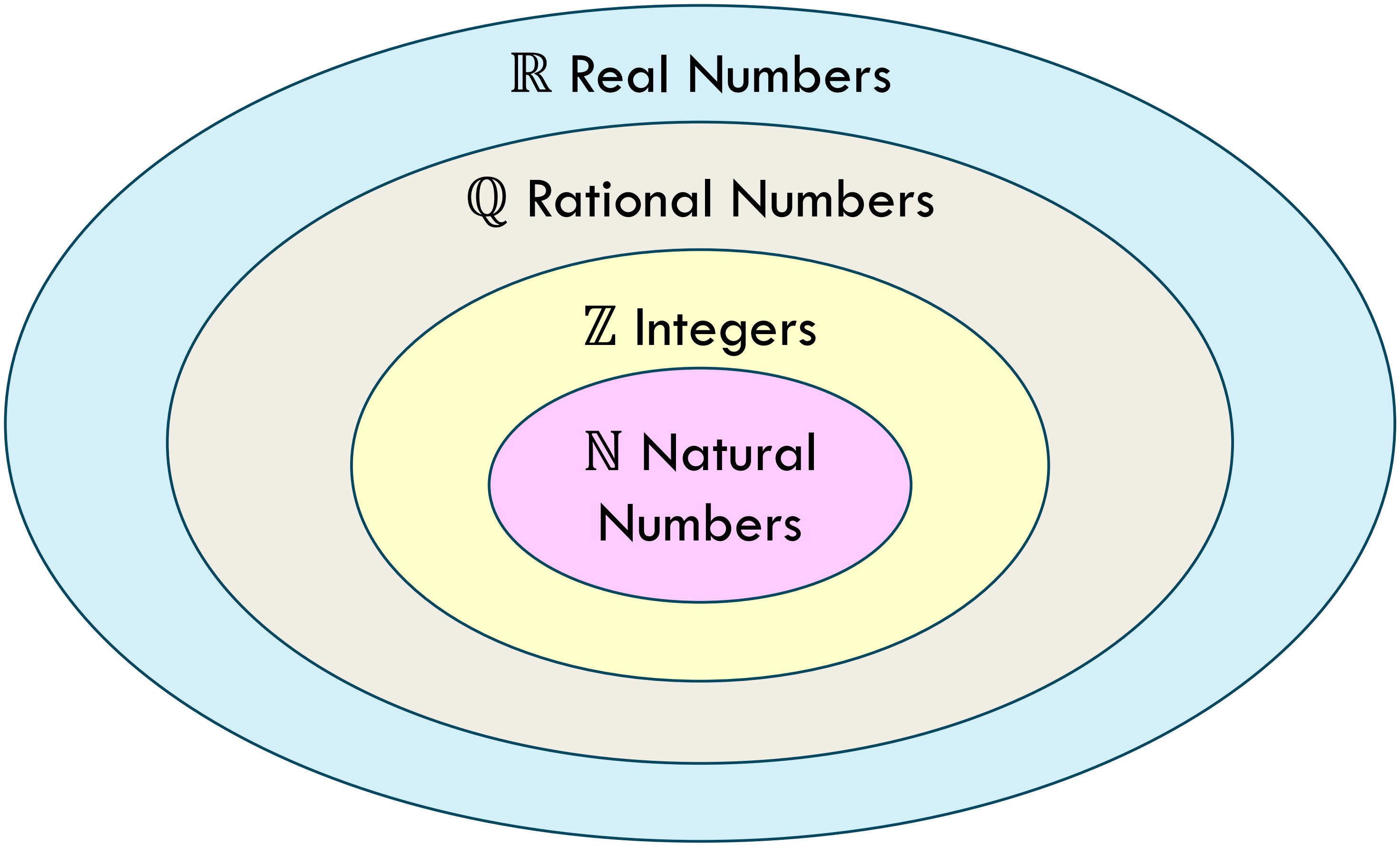
- We'll write a set as a collection of elements inside curly braces {}.
- Sets are often given variable names with capital letters.

- $A = \{0,5,8,10\} = \{5,8,0,10\}$ Sets are unordered
- $B = \{\text{watermelon}, \text{apple}, \text{pineapple}\}$ Sets can contain any object
- $C = \{a, b, c, c, b, a\} = \{a, b, c\}$ Repeat elements are listed once
- $D = \{0,1,2,3,4,5, \dots\}$ Sets can be finite or infinite

Common Sets

- $\mathbb{R}$ is the set of Real Numbers. E.g. $1, -17, \pi, \sqrt{2}$
- $\mathbb{Z}$ is the set of Integers. $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$
- $\mathbb{N}$ is the set of Natural Numbers. $\mathbb{N} = \{0, 1, 2, 3, \dots\}$
- $\mathbb{Q}$ is the set of Rational Numbers (fractions) E.g. $\frac{1}{2}, -\frac{11}{3}, 17$
- $\emptyset = \{\}$ is the Empty Set $\emptyset$ has no elements

Common Sets


ℝ Real Numbers
ℚ Rational Numbers
ℤ Integers
ℕ Natural Numbers

Sets can be elements of other sets

- For example:
- $A = \{\{1\}, \{2\}, \{1,2\}, \emptyset\}$
- $B = \{1, 2\}$

- Then $1 \in B, 2 \in B$. And $\emptyset \in A, B \in A$.

Sets Builder Notation

- Another way to describe a set is using set-builder notation.

- $S = \{x : \mathrm{P}(x)\}$ means S is the set of all x for which $\mathrm{P}(x)$ is true.

- For example:
- $\{x \in \mathbb{Z} : x > 0\}$ is the set of all positive integers.

- $\{x \in \mathbb{N} : x \equiv_3 2\}$ is the set $\{2, 5, 8, 11, 14, \ldots\}$.

- $\left\{\frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0\right\}$ is the set of rational numbers.

Set Cardinality

- The cardinality of a set is the number of elements in a set (its size). The cardinality of a set A is often denoted $|A|$.

- What is the cardinality of the following sets?
- $A = \{x \in \mathbb{Z} \,:\, x \equiv_4 1 \text{ and } -10 \leq x \leq 10\} = \{-7, -3, 1, 5, 9\}$
  $|\mathrm{A}| = 5$

- $B = \emptyset$
  $|\mathrm{B}| = 0$

- $C = \{\emptyset\}$
  $|C| = 1$

Relationships Between Sets

Set Equality

- Sets A and B are equal if they have the same elements.

- In predicate logic, $A = B$ is defined as:
- $\forall x \, (x \in A \leftrightarrow x \in B)$

A = {1, 2, 3}
B = {3, 4, 5}
C = {3, 4}
D = {4, 3, 3}
E = {3, 4, 3}
F = {4, {3}}

Which sets are equal?

$C = D = E$

Subset

- Set A is a subset of B if every element of A is also in B.

- In predicate logic, $A \subseteq B$ is defined as:
- $\forall x(x \in A \rightarrow x \in B)$

A = {1, 2, 3}
B = {3, 4, 5}
C = {3, 4}
D = {4, 3, 3}
E = {3, 4, 3}
F = {4, {3}}

Which sets are subsets?

$C \subseteq B$, $D \subseteq E$, $E \subseteq D$, etc.

Sets

Be careful about these two operations:

If $A = \{1,2,3,4,5\}$

$\{1\} \subseteq A$, but $\{1\} \notin A$

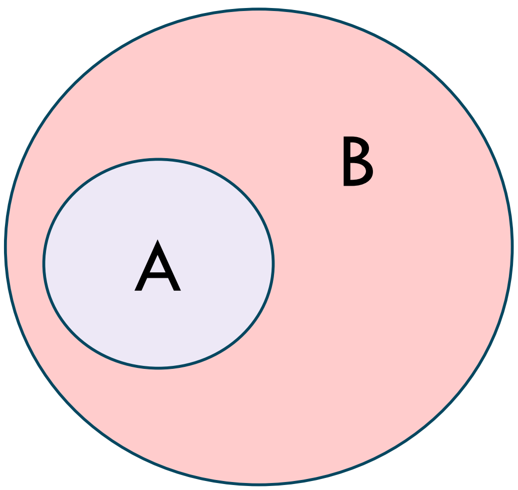
$\in$ asks: is this item in that box?

$\subseteq$ asks: is everything in this box also in that box?

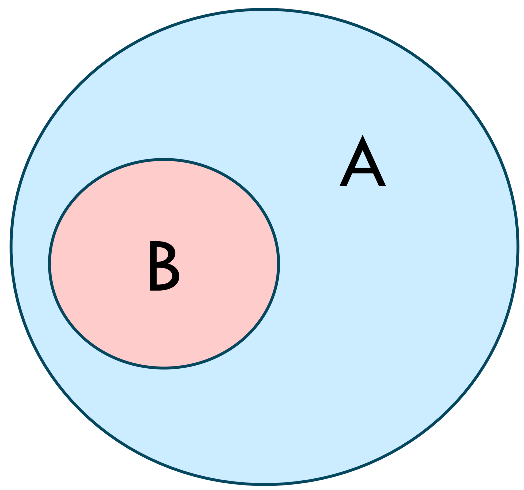
Set Equality and Subsets

- $A = B \equiv A \subseteq B \land B \subseteq A$

A is a subset of B



B is a subset of A



$\in$ vs. $\subseteq$

- $A = \{1, 2, 3\}$ $B = \{2\}$ $C = \{\emptyset, \{2\}\}$

- $\emptyset \subseteq A$? Yes.
- $\emptyset \in A$? No. $\emptyset \in C$ though!
- $2 \subseteq B$? No. $\{2\} \subseteq B$ though!
- $2 \in B$? Yes.
- $B \in A$? No. $B \subseteq A$ though!
- $B \in C$? Yes.

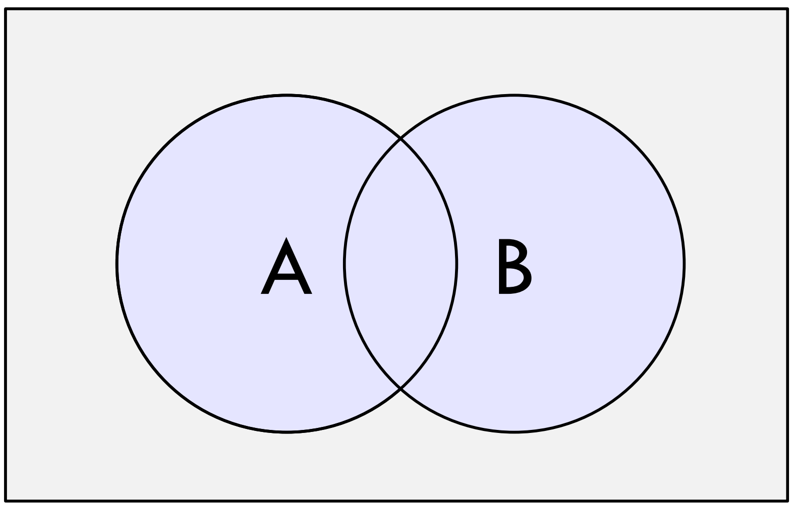
Set Operations

Combining Sets

Set Operations

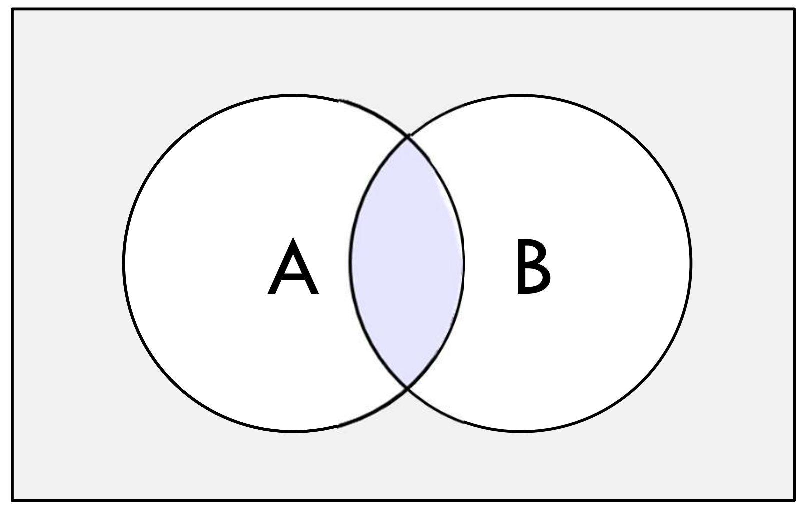
Union: $A \cup B$

$A \cup B = \{x : x \in A \vee x \in B\}$



Intersection: $A \cap B$

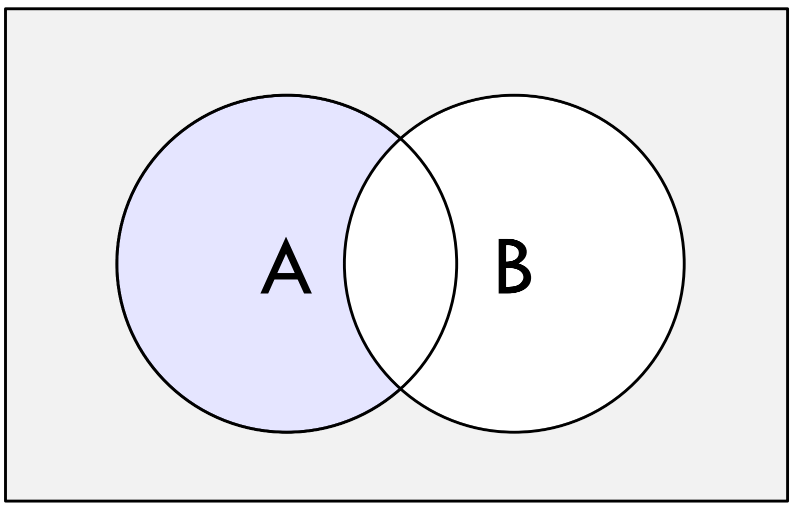
$A \cap B = \{x : x \in A \wedge x \in B\}$



Set Operations

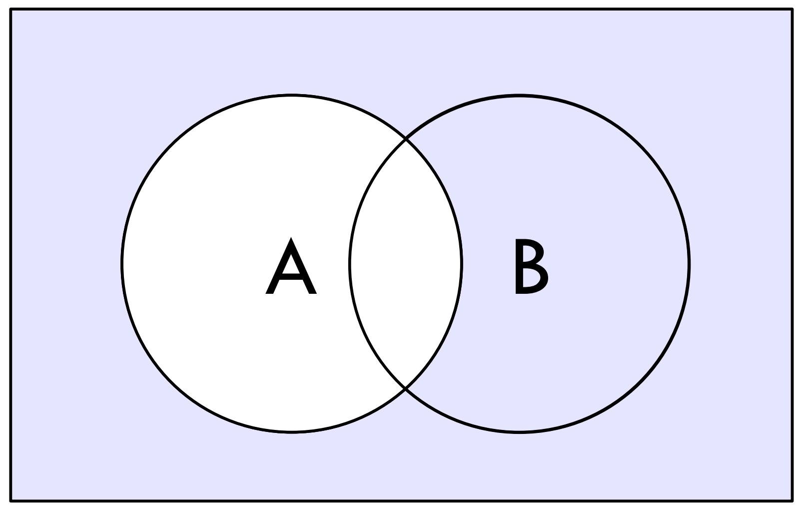
Set Difference: $A \setminus B$

$A \setminus B = \{x : x \in A \wedge x \notin B\}$

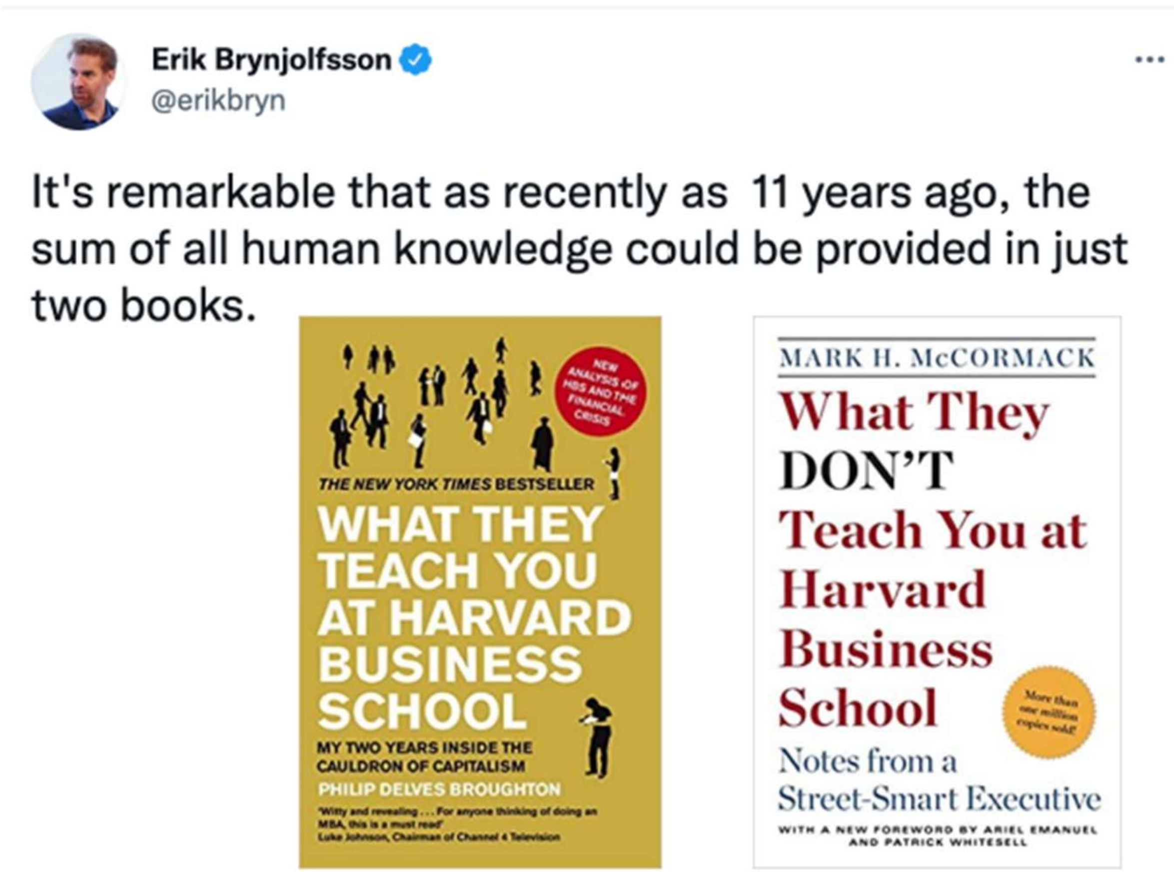


Set Complement: $\bar{A} = A^c$
(with respect to the universe $\mathcal{U}$)

$\bar{A} = \{x \in \mathcal{U}: x \notin A\}$



Set Operations



Exercises

Definitions
$A \cup B = \{x : x \in A \vee x \in B\}$
$A \cap B = \{x : x \in A \wedge x \in B\}$
$A \setminus B = \{x : x \in A \wedge x \notin B\}$
$\bar{A} = \{x : x \notin A\}$

- $A = \{1, 2, 3\}$ $B = \{3, 5, 6\}$ $C = \{3, 4\}$

- Using only A, B, C and set operations, make the following sets. The universe is all integers.

- $\{1, 2, 3, 4, 5, 6\} = A \cup B \cup C$

- $\{3\} = A \cap B$

- $\{1, 2\} = A \setminus B = A \cap \bar{B}$

Powerset

Powerset: $\mathcal{P}\{A\}$

$\mathcal{P}(A) = \{X : X \subseteq A\}$

The powerset of A is the **set** of all subsets of A.

$\mathcal{P}(\{1,2\}) = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}$

$\mathcal{P}(\{a, b, c\}) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$

Cartesian Product

Cartesian Product: $A \times B$

$A \times B = \{(a, b) : a \in A, b \in B\}$

The cartesian product of A with B is the set of ordered pairs of the form (a, b), where $a \in A$ and $b \in B$.

If $A = \{1,2\}$ and $B = \{a, b, c\}$ then:

$A \times B = \{(1, a), (1, b), (1, c), (2, a), (2, b), (2, c)\}$

$\mathbb{R} \times \mathbb{R} =$ the real plane. This is often denoted $\mathbb{R}^2$.

Exercises

Compute the following:

$\{1,2\} \times \emptyset = \emptyset$

$\mathcal{P}(\{2\} \times \{1,3\}) = \{\emptyset, \{(2,1)\}, \{(2,3)\}, \{(2,1), (2,3)\}\}$

$\mathcal{P}(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$

$|\mathcal{P}(\{1,2\}) \times \mathcal{P}(\{3,4,5\})| = 32$

Set Proofs

Two Claims

Determine if the following claims are true or false.

Claim 1: For all sets A, B, C, if $A \subseteq (B \cup C)$ then $A \subseteq B$ or $A \subseteq C$.

False.

Claim 2: For all sets A, B, C it holds that $A \cap B \cap C \subseteq A \cup B$.

True.

Claim 1

Claim 1: For all sets A, B, C, if $A \subseteq (B \cup C)$ then $A \subseteq B$ or $A \subseteq C$.

We disprove this claim. Let $A = \{1,2\}$, let $B = \{1\}$ and $C = \{2\}$. Then $A \subseteq (B \cup C)$, but $A \nsubseteq B$ and $A \nsubseteq C$.

Claim 2

Definition
$A \subseteq B \equiv \forall x(x \in A \rightarrow x \in B)$

Claim 2: For all sets A, B, C it holds that $A \cap B \cap C \subseteq A \cup B$.

Proof Strategy

- Let A, B, C be arbitrary sets.
- Let $x \in A \cap B \cap C$ be arbitrary.
- Prove that $x \in A \cup B$.

Claim 2

Definition
$A \subseteq B \equiv \forall x(x \in A \rightarrow x \in B)$

Claim 2: For all sets A, B, C it holds that $A \cap B \cap C \subseteq A \cup B$.

Proof

Let sets A, B, C be arbitrary. Let $x \in A \cap B \cap C$ be an arbitrary element. Then by definition of intersection, $x \in A$ and $x \in B$ and $x \in C$. Then certainly $x \in A$. So $x \in A$ or $x \in B$. So by definition of union, $x \in A \cup B$. Since x was arbitrary, $A \cap B \cap C \subseteq A \cup B$.