START RECORDING

Techniques of proof

Proving *universal / Existential statements* ***true*** *or* ***false***
Direct *and* ***indirect*** *proof strategies*

Basic definitions:Parity

- An integer n is called **even** if, and only if, there exists an integer k such that $n = 2k$.
- An integer n is called **odd** if, and only if, it is not even.
- Corollary: An integer n is called odd if, and only if, there exists an integer k such that $n = 2k + 1$
- The property of an integer as being either odd or even is known as its **parity**.
- n is odd if, and only if, $n \equiv 1 \ (mod\ 2)$ (resp, even, iff $n \equiv 0 \ (mod\ 2)$)

Arguing the positive: Universal Statements

- Let’s consider the following statement:

“The sum of an odd and an even integer is odd.”

Arguing the positive: Universal Statements

- Let's consider the following statement:

"The sum of an odd and an even integer is odd."

- Do you believe this statement?

Yes

No

Arguing the positive: Universal Statements

- Let's consider the following statement:

"The sum of an odd and an even integer is odd."

- Do you believe this statement?

Yes | No

- If you believe it, **you have to try to prove** that it's true (argue the positive/affirmative)

Proof

- Let x be even, then $x \equiv 0 \ (mod\ 2)$
- Let y be odd, then $y \equiv 1 \ (mod\ 2)$
- Consequently, $x + y \equiv 0 + 1 \equiv 1 \ (mod\ 2)$

Statements of claims / theorems

- Mathematical claims and theorems can be stated in various different ways!

“The sum of an odd and an even integer is odd.”

⇕

*“**Any two** integers of **opposite parity** sum to an **odd** number”*

⇕

*“**Every pair of** integers of **opposite parity** sums to an **odd** number”*

⇕

$$(\forall n_1 \in \mathbb{Z}^{2k+1})(\forall n_2 \in \mathbb{Z}^{2k})[\, n_1 + n_2 \in Z^{2k+1}]$$

Here’s some more!

- Let’s prove the following claims **true**:

1. The square of an odd integer is also odd.

Here's some more!

- Let's prove the following claims **true**:

1. The square of an odd integer is also odd.
2. If a is an integer, then $a^2 + a$ is even.

Here's some more!

- Let's prove the following claims **true**:

1. The square of an odd integer is also odd.
2. If a is an integer, then $a^2 + a$ is even.
3. *If m is an even integer and n is an odd integer,* $m^2 + 3n$ *is odd.*

Here's some more!

- Let's prove the following claims **true**:

1. The square of an odd integer is also odd.
2. If a is an integer, then $a^2 + a$ is even.
3. *If m is an even integer and n is an odd integer,* $m^2 + 3n$ *is odd.*
4. *If n is odd,* $n^2 = 8m + 1$ *for some integer* m.

Here's some more!

- Let's prove the following claims **true**:

1. The square of an odd integer is also odd.
2. If a is an integer, then $a^2 + a$ is even.
3. *If m is an even integer and n is an odd integer,* $m^2 + 3n$ *is odd.*
4. *If n is odd,* $n^2 = 8m + 1$ *for some integer* m.
5. If a, b are ***rationals,*** $^{(a+b)}/_{2}$ is also rational

Arguing the negative: counter-example

- Since

$$(\sim \forall x \in D)[P(x)] \equiv (\exists x \in D)[\sim P(x)]$$

- x is referred to as a *counter-example*.

- Examples:
  a) *All primes are odd.*

Arguing the negative: counter-example

- Since

$$(\sim \forall x \in D)[P(x)] \equiv (\exists x \in D)[\sim P(x)]$$

- x is referred to as a *counter-example*.

- Examples:
  a) *All primes are odd.* **Disproof by counter-example:**
     1. All primes are odd.
        Counter-example: 2 is prime but also even.

Arguing the negative: counter-example

- Since

$$\sim (\forall x \in D)[P(x)] \equiv (\exists x \in D)[\sim P(x)]$$

- x is referred to as a *counter-example*.

- Examples:
  b) The tenths and units digits of all perfect squares 16 and above have an absolute difference bigger than 1.

Arguing the negative: counter-example

- Since

$$\sim (\forall x \in D)[P(x)] \equiv (\exists x \in D)[\sim P(x)]$$

- x is referred to as a *counter-example*.
- Examples:

  b) The tens and ones digits of all perfect squares 16 and above have an absolute difference bigger than 1. Disproof by counterexample:

  1. 100 is a perfect square ≥ 16, since $\sqrt{100} = 10 \in \mathbb{Z}$.
  2. The ones **and** tenths digits of 100 are 0.
  3. $0 - 0 = 0 < 1.$
  4. By (1), (2), (3), we have that 100 is a counter-example.
  5. Therefore, the statement is **false**. Done.

Perfect Squares

- Consider perfect square 16 or greater whose *units* and *tenths* digits have an absolute difference of less than 4.

n	n^2	|Ten - Unit|
4	16	5
5	25	3
6	36	3

Perfect Squares

- $\forall x \geq 4$ $[x^2$ has a difference of tens and units be $< 4]$

Perfect Squares

- $\forall x \geq 4\ [x^2$ has diff of tens and units be $< 4]$
- False!

- Counterexample: 4^2

Perfect Squares

- $\forall x \geq 4$ $[x^2$ has diff of tens and units be $< 4]$
- False!

- Counterexample: 4^2

- $\forall x \geq 5$ $[x^2$ has diff of tens and units be $< 4]$

Perfect Squares

- $\forall x \geq 5\ [x^2$ has diff of tens and units be $< 4]$

n	n^2	|Ten - Unit|
20	400	0
21	441	3
22	484	4
23	529	7
24	576	1
25	625	3

n	n^2	|Ten - Unit|
26	676	1
27	729	7
28	784	4
29	841	3
30	900	0

Perfect Squares

- $\forall x \geq 5\ [x^2$ has diff of tens and units be $< 4]$
- False!

- Counterexample: 22^2

Perfect Squares

- $\forall x \geq 5\ [x^2$ has diff of tens and units be $< 4]$
- False!

- Counterexample: 22^2

- $\forall x \geq 29\ [x^2$ has diff of tens and units be $< 4]$

Perfect Squares

- $\forall x \geq 5\ [x^2$ has diff of tens and units be $< 4]$
- False!

- Counterexample: 22^2

- $\forall x \geq 29\ \left[x^2 \right.$ has diff of tens and units be $\left. < 4\right]$
  - Don’t know. On a HW will ask you to write a program to see what happens up to 1000.

Arguing the affirmative of existential statements

- Two methods:
  1. **Constructive**
  2. **Non-Constructive**
- In “constructive” proofs we either **explicitly** show or **construct** an element of the domain that answers our query.
- In **non-constructive** proofs (very rare in this class) we prove that **it is a logical necessity** for such an element to exist!
  - But we neither explicitly, nor implicitly, show or construct such an element!

Constructive proofs in Number Theory (and one non-constructive one)

Our first constructive proof

- **Claim**: There exists a natural number that you ***cannot*** write as a sum of three squares of natural numbers.
  - Examples of numbers you ***can*** write as a sum of three squares:
    - $0 = 0^2 + 0^2 + 0^2$
    - $1 = 1^2 + 0^2 + 0^2$
    - $2 = 1^2 + 1^2 + 0^2$
- Try to find a number that ***cannot*** be written as such.

Proof

- The natural number 7 cannot be written as the sum of three squares.
- This we can prove by case analysis:
  1. Can't use 3, since $3^2 = 9 > 7$
  2. Can't use 2 more than once, since $2^2 + 2^2 = 8 > 7$
  3. So, we can use 2, one or zero times.
     a) If we use 2 once, we have $7 = 2^2 + a^2 + b^2 \leq 2^2 + 1^2 + 1^2 = 6 < 7$
     b) If we use 2 zero times, the maximum value is $1^2 + 1^2 + 1^2 = 3 < 7$
  4. Done!

Sum of Three Squares

- In Breakout Rooms, Find:
  - Other numbers that are NOT the sum of 3 squares
  - Try to prove there are an INFINITE number of numbers that are NOT the sum of 3 squares

Sum of Three Squares

- If $n \equiv 7 \ (mod\ 8)$, then n CANNOT be written as the sum of 3 squares

Mod 8	
$0^2 \equiv 0$	$4^2 \equiv 0$
$1^2 \equiv 1$	$5^2 \equiv 1$
$2^2 \equiv 4$	$6^2 \equiv 4$
$3^2 \equiv 1$	$7^2 \equiv 1$

Sum of Three Squares

So, is there some way for three numbers from 0, 1, 4 to add up to $7(mod\ 8)$?

Case 1: Use *zero* 4's. Then max is 1+1+1≡3 < 7.

Case 2: Use exactly *one* 4. Then we have to get 3 with two of {0,1}, but the max is 1+1 ≡ 2 < 4.

Case 3: Use *two* 4's 4+4+0=1, 4+4+1 ≡ 2.

Case 4: Use *three* 4's 4+4+4 ≡ 4.

Your turn, class!

- Let’s break into breakout rooms and prove the following theorems:

1. There exists an integer n that can be written in ***two ways*** (i.e ***at least one*** of the two summands is ***different***) as a sum of two prime numbers.
2. There is a **perfect square** that can be written as a sum of two other **perfect squares**.
3. Suppose $r, s \in \mathbb{Z}$. Then, $(\exists k \in \mathbb{Z})[\,22r + 18s = 2k]$

Your turn, class!

- Let's split in teams and prove the following theorems:

1. There exists an integer n that can be written in ***two ways*** (i.e ***at least one*** of the two summands is ***different***) as a sum of two prime numbers.
2. There is a **perfect square** that can be written as a sum of two other **perfect squares**.
3. Suppose $r, s \in \mathbb{Z}$. Then, $(\exists k \in \mathbb{Z})[\,22r + 18s = 2k]$

How is the 3rd proof different from the others?

Our first non-constructive proof

- **Theorem**: There exists a pair of irrational numbers a and b such that a^b is a rational number.

Our first non-constructive proof

- For the following proof, we will assume *known* that $\sqrt{2} \notin \mathbb{Q}$.
- This is a *fact*, which we will prove later on in this section.
- Now, on to the proof!

Our first non-constructive proof

- **Theorem**: There exists a pair of irrational numbers a and b such that a^b is a rational number.

Our first non-constructive proof

- **Theorem**: There exists a pair of irrational numbers a and b such that a^b is a rational number.
- **Proof**: Let $a = b = \sqrt{2}$. Since $\sqrt{2}$ is irrational, a and b are both irrational. Is $a^b = (\sqrt{2})^{\sqrt{2}}$ **rational**? Two cases:

Our first non-constructive proof

- **Theorem**: There exists a pair of irrational numbers a and b such that a^b is a rational number.
- **Proof**: Let $a = b = \sqrt{2}$. Since $\sqrt{2}$ is irrational, a and b are both irrational. Is $a^b = (\sqrt{2})^{\sqrt{2}}$ **rational**? Two cases:
  1. If $\sqrt{2}^{\sqrt{2}}$ is rational, then we have proven the result. Done.

Our first non-constructive proof

- **Theorem**: There exists a pair of irrational numbers a and b such that a^b is a rational number.
- **Proof**: Let $a = b = \sqrt{2}$. Since $\sqrt{2}$ is irrational, a and b are both irrational. Is $a^b = (\sqrt{2})^{\sqrt{2}}$ **rational**? Two cases:
  1. If $\sqrt{2}^{\sqrt{2}}$ is rational, then we have proven the result. Done.
  2. If $\sqrt{2}^{\sqrt{2}}$ is irrational, then we will name it c. Then, observe that $c^{\sqrt{2}}$ is rational, since $c^{\sqrt{2}} = \left(\left(\sqrt{2}\right)^{\sqrt{2}}\right)^{\sqrt{2}} = \left(\sqrt{2}\right)^2 = 2 \in \mathbb{Q}$. Since both c and $\sqrt{2}$ are irrationals, but $c^{\sqrt{2}}$ is rational, we are done.

Analysis of proof

- Suppose $x = \sqrt{2},$ an irrational. From the previous theorem, we know:
  a) Either that $a = x, b = x$ are two irrationals that satisfy the condition , OR
  b) That $a = x^x, b = x$ are the two irrationals.

- But we **don’t care which pair it is**! As long as one exists!

Indirect Proofs of Number Theory

- Sometimes, proving a fact ***directly*** is tough.
- In such cases, we can attempt an ***indirect*** proof
- Those are split in two categories:
    1. Proofs by contraposition
    2. Proofs by contradiction
- We will see examples of both.

Proof by contraposition

- Applicable to all kinds of statements of type:

$$(\forall x \in D)[P(x) \Rightarrow Q(x)]$$

- Sometimes, proving the implication in this way can be **hard**.
- On the other hand, proving its ***contrapositive:***

$$(\forall x \in D)[\sim Q(x) \Rightarrow \sim P(x)]$$

might be easier! ☺

Examples

- $(\forall a \in \mathbb{Z})\left[(a^2\ even) \Rightarrow (a\ even)\right]$

Examples

- $(\forall a \in \mathbb{Z})[(a^2\ even) \Rightarrow (a\ even)]$
- Do we believe this to be true?

Yes

No

Examples

- $(\forall a \in \mathbb{Z})\left[(a^2\ even) \Rightarrow (a\ even)\right]$
- Do we believe this to be true?

Yes | No

- So we should aim for a proof of the **affirmative**!

Examples

- $(\forall a \in \mathbb{Z})\left[(a^2\ even) \Rightarrow (a\ even)\right]$
- Proving this ***directly*** is somewhat hard
- On the other hand, the **contrapositive**:

$$(\forall a \in \mathbb{Z})[\ (a\ odd) \Rightarrow (a^2\ odd\ )]$$

is **much easier**!

Proof that $(\forall a \in \mathbb{Z})[\ (a\ odd) \Rightarrow (a^2\ odd\ )]$

1. Suppose a is an odd integer.
2. Then, $a \equiv 1\ (mod\ 2)$.
3. By algebra, $a^2 \equiv 1^2 \equiv 1\ (mod\ 2)$.
4. Done.

Another example

If $3n + 2$ is odd, where $n \in \mathbb{Z}$, then n is odd.

Another example

If $3n + 2$ is odd, where $n \in \mathbb{Z}$, then n is odd.

Let's try this one together.

Another example

If $n = a \cdot b$, where $a, b \in \mathbb{N}^{\geq 1}$, then $a \leq \sqrt{n}$ OR $b \leq \sqrt{n}$

Another example

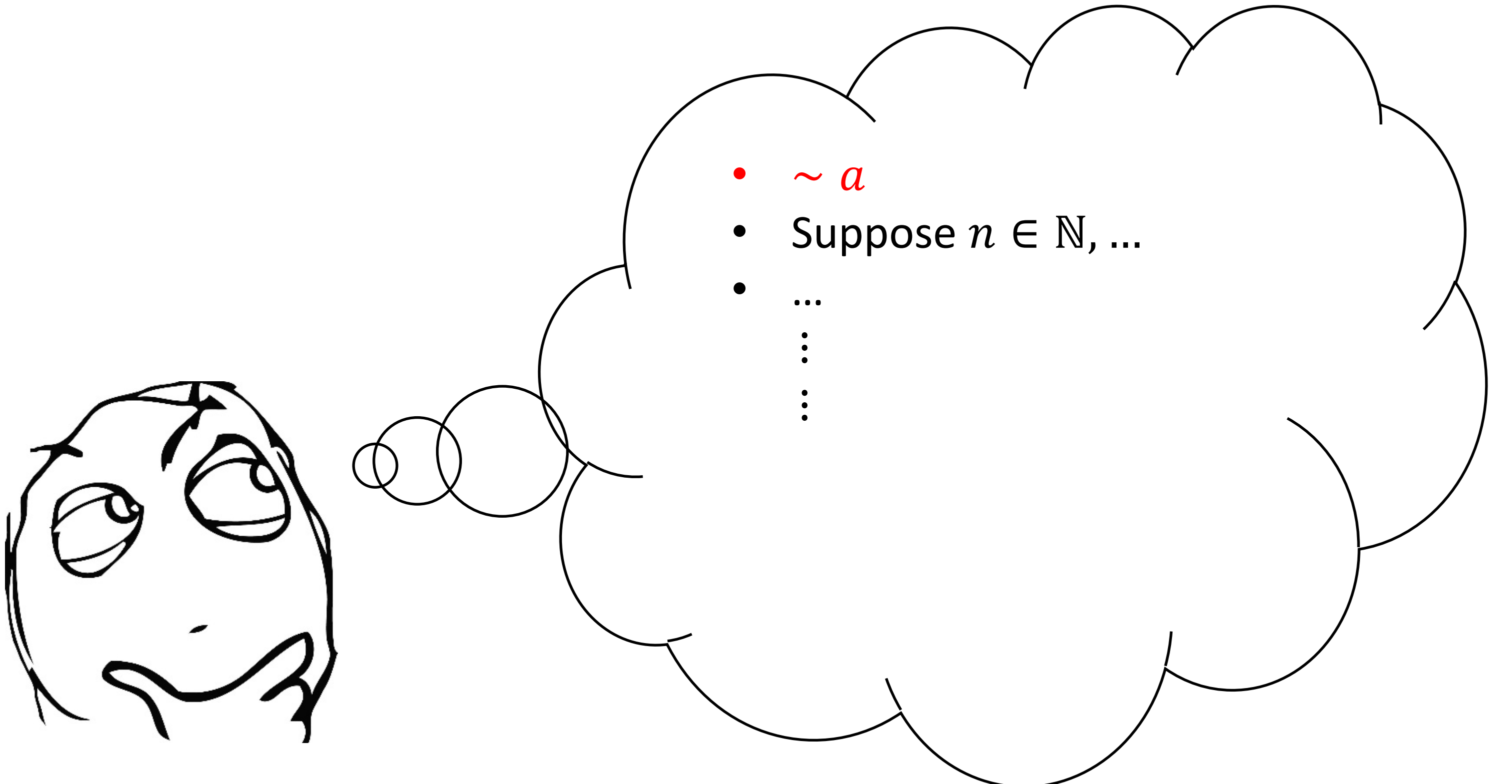
If $n = a \cdot b$, where $a, b \in \mathbb{N}^{\geq 1}$, then $a \leq \sqrt{n}$ OR $b \leq \sqrt{n}$

Proof by contradiction

- The most common type of indirect proof is *proof by contradiction*
- Briefly: We want to prove a fact a, so **we assume $\sim \boldsymbol{a}$** and **hope that we reach a contradiction** (a falsehood).

Proof by contradiction

- The most common type of indirect proof is *proof by contradiction*
- Briefly: We want to prove a fact a, so **we assume $\sim a$** and **hope that we reach a contradiction** (a falsehood).



This is a so-called **"conditional world"**: It's a "version" of our world **where we assume $\sim a$.**

Proof by contradiction

- The most common type of indirect proof is *proof by contradiction*
- Briefly: We want to prove a fact a, so **we assume $\sim a$** and **hope that we reach a contradiction** (a falsehood).

- $\sim a$
- Suppose $n \in \mathbb{N}$, ...
- ...

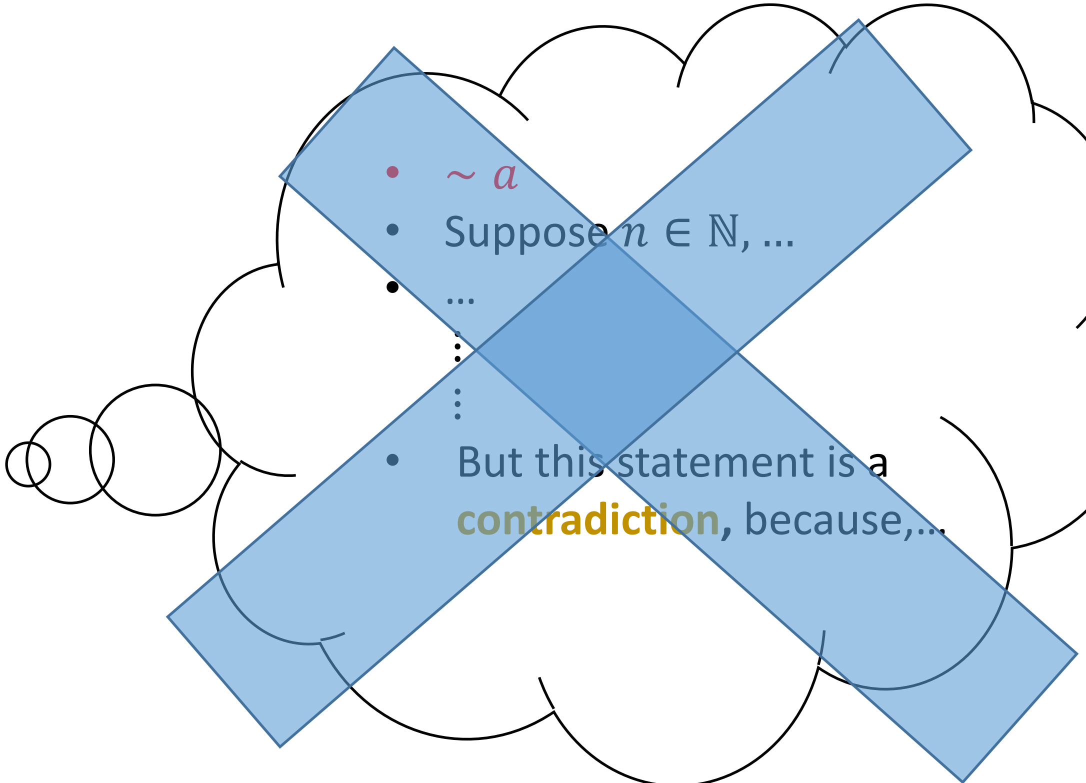
  $\vdots$

  $\vdots$
- But this statement is a **contradiction**, because,...

We follow some classic direct proof sets, and reach a statement that is a **logical contradiction!** *(e.g 1 > 2)*

Proof by contradiction

- The most common type of indirect proof is *proof by contradiction*
- Briefly: We want to prove a fact a, so **we assume $\sim a$** and **hope that we reach a contradiction** (a falsehood).

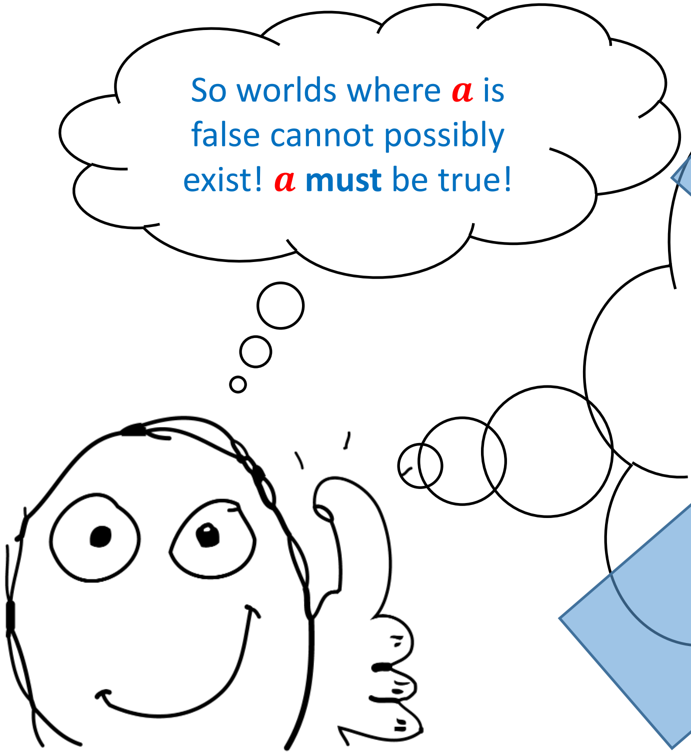


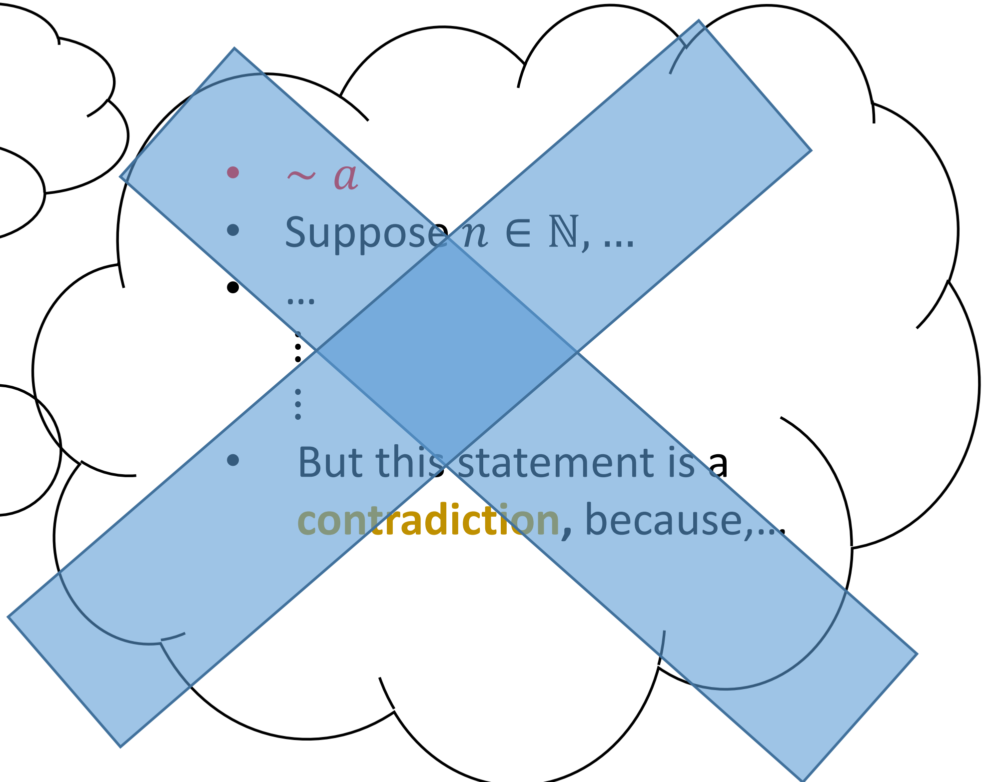
We follow some classic direct proof sets, and reach a statement that is a **logical contradiction!** *(e.g 1 > 2)*

This means that this conditional world cannot possibly exist! The only "possible" worlds have a in it.

Proof by contradiction

- The most common type of indirect proof is *proof by contradiction*
- Briefly: We want to prove a fact a, so **we assume $\sim a$** and **hope that we reach a contradiction** (a falsehood).





We follow some classic direct proof sets, and reach a statement that is a **logical contradiction!** *(e.g 1 > 2)*

This means that this conditional world cannot possibly exist! The only "possible" worlds have a in it.

Proof by contradiction

- Proof of contradiction is often used in statements that *look obvious!*
- Example: **We will prove that there is no greatest integer.**

Proof by contradiction

- Proof of contradiction is often used in statements that *look obvious!*
- Example: **We will prove that there is no greatest integer.**
- Proof:
  1. ***Assume that the statement is false.*** Then, there is a greatest integer.
  2. Call the integer assumed in step 1 N.
  3. By closure of $\mathbb{Z}$ over addition, we have that $N + 1 \in \mathbb{Z}$.
  4. But $N + 1 > N$.
  5. Steps 4 and 1 are a contradiction. Therefore, there does **not** exist a greatest integer.

Your turn!

- Prove that the square root of any **irrational** is **also** irrational

A historical proof by contradiction: $\sqrt{2}$ is irrational

A historical proof by contradiction: $\sqrt{2}$ is irrational

1. Let's assume BY WAY OF CONTRADICTION that $\sqrt{2}$ is rational.

A historical proof by contradiction: $\sqrt{2}$ is irrational

1. Let's assume BY WAY OF CONTRADICTION that $\sqrt{2}$ is rational.
2. So $\sqrt{2} = \frac{a}{b}$, $a, b \in \mathbb{Z}, b \neq 0$ and a, b do not have common factors.

A historical proof by contradiction: $\sqrt{2}$ is irrational

1. Let's assume BY WAY OF CONTRADICTION that $\sqrt{2}$ is rational.
2. So $\sqrt{2} = \frac{a}{b}$, $a, b \in \mathbb{Z}, b \neq 0$ and a, b do not have common factors.
3. So $a = \sqrt{2} \cdot b \Rightarrow a^2 = 2b^2$ so a^2 is even **(1)**

A historical proof by contradiction: $\sqrt{2}$ is irrational

1. Let's assume BY WAY OF CONTRADICTION that $\sqrt{2}$ is rational.
2. So $\sqrt{2} = \frac{a}{b}$, $a, b \in \mathbb{Z}, b \neq 0$ and a, b do not have common factors.
3. So $a = \sqrt{2} \cdot b \Rightarrow a^2 = 2b^2$ so a^2 is even **(1)**
4. By the theorem proved before, this means that a is even.

A historical proof by contradiction:
$\sqrt{2}$ is irrational

1. Let's assume BY WAY OF CONTRADICTION that $\sqrt{2}$ is rational.
2. So $\sqrt{2} = \frac{a}{b}$, $a, b \in \mathbb{Z}, b \neq 0$ and a, b do not have common factors.
3. So $a = \sqrt{2} \cdot b \Rightarrow a^2 = 2b^2$ so a^2 is even **(1)**
4. By the theorem proved before, this means that a is even.
5. So $a = 2k$ for some integer k. **(2)**

A historical proof by contradiction: $\sqrt{2}$ is irrational

1. Let's assume BY WAY OF CONTRADICTION that $\sqrt{2}$ is rational.
2. So $\sqrt{2} = \frac{a}{b}$, $a, b \in \mathbb{Z}, b \neq 0$ and a, b do not have common factors.
3. So $a = \sqrt{2} \cdot b \Rightarrow a^2 = 2b^2$ so a^2 is even **(1)**
4. By the theorem proved before, this means that a is even.
5. So $a = 2k$ for some integer k. **(2)**
6. Substituting **(2)** into **(1)** yields: $(2k)^2 = 2b^2 \Rightarrow b^2 = 2k^2 \Rightarrow$

A historical proof by contradiction: $\sqrt{2}$ is irrational

1. Let's assume BY WAY OF CONTRADICTION that $\sqrt{2}$ is rational.
2. So $\sqrt{2} = \frac{a}{b}$, $a, b \in \mathbb{Z}, b \neq 0$ and a, b do not have common factors.
3. So $a = \sqrt{2} \cdot b \Rightarrow a^2 = 2b^2$ so a^2 is even **(1)**
4. By the theorem proved before, this means that a is even.
5. So $a = 2k$ for some integer k. **(2)**
6. Substituting **(2)** into **(1)** yields: $(2k)^2 = 2b^2 \Rightarrow b^2 = 2k^2 \Rightarrow$
7. b^2 is even $\Rightarrow$ b is even by previous theorem!

A historical proof by contradiction: $\sqrt{2}$ is irrational

1. Let's assume BY WAY OF CONTRADICTION that $\sqrt{2}$ is rational.
2. So $\sqrt{2} = \frac{a}{b}$, $a, b \in \mathbb{Z}, b \neq 0$ and a, b do not have common factors.
3. So $a = \sqrt{2} \cdot b \Rightarrow a^2 = 2b^2$ so a^2 is even **(1)**
4. By the theorem proved before, this means that a is even.
5. So $a = 2k$ for some integer k. **(2)**
6. Substituting **(2)** into **(1)** yields: $(2k)^2 = 2b^2 \Rightarrow b^2 = 2k^2 \Rightarrow$
7. b^2 is even $\Rightarrow$ b is even by previous theorem!
8. So both a and b are both even, which means that they have common factor of 2.

A historical proof by contradiction: $\sqrt{2}$ is irrational

1. Let's assume BY WAY OF CONTRADICTION that $\sqrt{2}$ is rational.
2. So $\sqrt{2} = \frac{a}{b}$, $a, b \in \mathbb{Z}, b \neq 0$ and a, b do not have common factors.
3. So $a = \sqrt{2} \cdot b \Rightarrow a^2 = 2b^2$ so a^2 is even **(1)**
4. By the theorem proved before, this means that a is even.
5. So $a = 2k$ for some integer k. **(2)**
6. Substituting **(2)** into **(1)** yields: $(2k)^2 = 2b^2 \Rightarrow b^2 = 2k^2 \Rightarrow$
7. b^2 is even $\Rightarrow$ b is even by previous theorem!
8. So both a and b are both even, which means that they have common factor of 2.
9. Contradiction.

Proof of a lemma

- Proof (via contraposition): We prove the contrapositive, i.e

If a^2 is a multiple of 5, then so is a

$$\Leftrightarrow$$

If a is not a multiple of 5, then a^2 isn't one either.

Proof of lemma

- Proof (by contraposition): We prove that:

if a is not a multiple of 5, then a^2 isn't one either.

Proof of lemma

- Proof (by contraposition): We prove that:

if a is not a multiple of 5, then a^2 isn't one either.

1. Suppose that $a \in \mathbb{Z}$ is **not** a multiple of 5.

Proof of lemma

- Proof (by contraposition): We prove that:

if a is not a multiple of 5, then a^2 isn't one either.

1. Suppose that $a \in \mathbb{Z}$ is **not** a multiple of 5.
2. Then, one of the following has to be the case (all $\equiv$ are mod 5):
   - $a \equiv 1 \Rightarrow a^2 \equiv 1^2 \equiv 1 \not\equiv 0$
   - $a \equiv 2 \Rightarrow a^2 \equiv 4 \equiv 4 \not\equiv 0$
   - $a \equiv 3 \Rightarrow a^2 \equiv 1^2 \equiv 1 \not\equiv 0$
   - $a \equiv 4 \Rightarrow a^2 \equiv 16 \equiv 1 \not\equiv 0$

Adjustment: Proof that $\sqrt{5}$ is irrational

- Let's assume BY WAY OF CONTRADICTION that $\sqrt{5}$ is rational.
- So $\sqrt{5} = \frac{a}{b},\ a, b \in \mathbb{Z}, b \neq 0$ and a, b do not have common factors.
- So $a = \sqrt{5} \cdot b \Rightarrow a^2 = 5b^2$ so a^2 is a multiple of 5 **(1)**
- By the previous theorem, this means that a is a multiple of 5.
- So $a = 5k$ for some integer k. **(2)**
- Substituting (2) into (1) yields: $(5k)^2 = 5b^2 \Rightarrow b^2 = 5k^2 \Rightarrow$
  b^2 is a multiple of 5 $\Rightarrow$ b is a multiple of 5 by same theorem
- Since a and b are both multiples of 5, they have a common factor of 5.
- Contradiction.

Proof of $\sqrt{7} \notin \mathbb{Q}$ with Euclidean Argument

Proof that $\sqrt{4}$ is irrational (???)

- Why can we **not** use this machinery to prove that $\sqrt{4}$ is irrational (which is wrong anyway)?

Proof that $\sqrt{4}$ is irrational (???)

- Why can we **not** use this machinery to prove that $\sqrt{4}$ is irrational (which is wrong anyway)?
- Observe that to prove $\sqrt{2}$ irrational, we needed lemma: x^2 even $\Rightarrow x$ even

Proof that $\sqrt{4}$ is irrational (???)

- Why can we **not** use this machinery to prove that $\sqrt{4}$ is irrational (which is wrong anyway)?
- Observe that to prove $\sqrt{2}$ irrational, we needed lemma: x^2 even $\Rightarrow x$ even.
- To prove $\sqrt{3}$ irrational, we need lemma: x^2 mult 3 $\Rightarrow x$ mult 3

Proof that $\sqrt{4}$ is irrational (???)

- Why can we **not** use this machinery to prove that $\sqrt{4}$ is irrational (which is wrong anyway)?
- Observe that to prove $\sqrt{2}$ irrational, we needed lemma: x^2 even $\Rightarrow x$ even.
- To prove $\sqrt{3}$ irrational, we need lemma: x^2 mult 3 $\Rightarrow x$ mult 3
- To prove $\sqrt{4}$ irrational, we would need lemma: x^2 mult 4 $\Rightarrow x$ mult 4.

Proof that $\sqrt{4}$ is irrational (???)

- Why can we **not** use this machinery to prove that $\sqrt{4}$ is irrational (which is wrong anyway)?
- Observe that to prove $\sqrt{2}$ irrational, we needed lemma: x^2 even $\Rightarrow x$ even.
- To prove $\sqrt{3}$ irrational, we need lemma: x^2 mult 3 $\Rightarrow x$ mult 3
- To prove $\sqrt{4}$ irrational, we would need lemma: x^2 mult 4 $\Rightarrow x$ mult 4.
- But this is **not** actually true! Counter-example: $x = 2$

Exercise

- Please go ahead and find the smallest possible positive factors for the following numbers (excluding the trivial factor 1):
    - 15
    - 22
    - 29
    - 121
    - 1024
    - 1027

Exercise

- Please go ahead and find the smallest possible positive factors for the following numbers (excluding the trivial factor 1):
  - $15 = 3 \times 5 = 3^1 \times 5^1$
  - $22 = 2^1 \times 11^1$
  - $29 = 29^1$
  - $121 = 11^2$
  - $1024 = 2^{10}$
  - $1027 = 13 \times 79 = 13^1 \times 79^1$

Exercise

- Please go ahead and find the smallest possible positive factors for the following numbers (excluding the trivial factor 1):
  - $15 = 3 \times 5 = 3^1 \times 5^1$
  - $22 = 2^1 \times 11^1$
  - $29 = 29^1$
  - $121 = 11^2$
  - $1024 = 2^{10}$
  - $1027 = 13 \times 79 = 13^1 \times 79^1$

What do all of these factors have in common?

Exercise

- Please go ahead and find the smallest possible positive factors for the following numbers (excluding the trivial factor 1):
  - $15 = 3 \times 5 = 3^1 \times 5^1$
  - $22 = 2^1 \times 11^1$
  - $29 = 29^1$
  - $121 = 11^2$
  - $1024 = 2^{10}$
  - $1027 = 13 \times 79 = 13^1 \times 79^1$

What do all of these factors have in common?

They are all primes!

A result

- Every positive integer $n \geq 2$ can be factored into a product of **exclusively** prime numbers

A result

- Every positive integer $n \geq 2$ can be factored into a product of **exclusively** prime numbers
- Moreover, this representation is ***unique***, up to re-ordering of the individual factors in the product! For example:
  - $15 = 3^1 \times 5^1 = 5^1 \times 3^1$
  - $1400 = 2^3 \times 5^2 \times 7^1 = 2^3 \times 7^1 \times 5^2 =$

$$= 5^2 \times 2^3 \times 7^1 = 5^2 \times 7^1 \times 2^3 =$$

$$= 7^1 \times 2^3 \times 5^2 = 7^1 \times 5^2 \times 2^3$$

Unique Prime Factorization Theorem

- Every number $n \in \mathbb{N}^{\geq 2}$ can be **uniquely** factored into a product of prime numbers $p_1, p_2, \dots, p_k$ like so:

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdot \dots \cdot p_k^{e_k}, \qquad e_i \in \mathbb{N}^{>0}$$

Unique Prime Factorization Theorem

- Every number $n \in \mathbb{N}^{\geq 2}$ can be **uniquely** factored into a product of prime numbers $p_1, p_2, \ldots, p_k$ like so:

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_k^{e_k}, \qquad e_i \in \mathbb{N}^{>0}$$

- Proving existence is easy

Unique Prime Factorization Theorem

- Every number $n \in \mathbb{N}^{\geq 2}$ can be **uniquely** factored into a product of prime numbers $p_1, p_2, \ldots, p_k$ like so:

$$n = p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_k^{e_k}, \qquad e_i \in \mathbb{N}^{>0}$$

- Proving existence is easy
- Proving uniqueness is harder

Examples of "uniqueness"

- By "uniqueness" we mean that the product is unique up to reordering of the factors $p_i^{e_i}$.
- Examples:
  - $30 = 3^1 \times 2^1 \times 5^1 = 5^1 \times 2^1 \times 3^1$
  - $88 = 2^3 \times 11^1 = 11^1 \times 2^3$
  - $1026 = 2^1 \times 3^3 \times 19^1 = 2^1 \times 19^1 \times 3^3 = 19^1 \times 2^1 \times 3^3 = 3^3 \times 19^1 \times 2^1$

A necessary lemma

Set of primes

- Claim: Let $p \in \mathbf{P}$, $a \in \mathbb{N}$. Then, if $p \mid a$, then $p \nmid (a+1)$.

A necessary lemma

Set of primes

- Claim: Let $p \in \mathbf{P}$, $a \in \mathbb{N}$. Then, if $p \mid a$, then $p \nmid (a+1)$.
- Proof:
  - Assume that $p \mid (a+1)$. Then, this means that $(\exists r_1 \in \mathbb{Z})[a+1 = p \cdot r_1]$ (I)
  - We already know that $p \mid a \Rightarrow (\exists r_2 \in \mathbb{Z})[a = p \cdot r_2]$ (II)
  - Substituting (II) into (I) yields: $p \cdot r_2 + 1 = p \cdot r_1 \Rightarrow p(r_1 - r_2) = 1 \Rightarrow p \mid 1$ which is a contradiction. Therefore, $p \nmid (a+1)$.

Infinity of primes

- Assume that the primes are finite. Then, we can list them in ascending order:

$$p_1, p_2, \dots, p_n$$

Infinity of primes

- Assume that the primes are finite. Then, we can list them in ascending order:

$$p_1, p_2, \dots, p_n$$

Let's consider the number

$$N = p_1 \cdot p_2 \cdot \dots \cdot p_n + 1$$

Infinity of primes

$$N = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$$

Clearly, N is bigger than any p_i. We have two cases:

i. *N* is prime. Contradiction, since N is bigger than any prime.

ii. *N* is composite. This means that N has at least one factor f. Let's take the smallest factor of *N*, and call it f_{min}. Then, this number is prime (why?)
Since f_{min} is prime, it divides $p_1 \cdot p_2 \cdot \ldots \cdot p_n$. By the previous theorem, this means that it cannot possibly divide $p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1 = N$.
Contradiction, since we assumed that f_{min} is a factor of N.

Therefore, the primes are not finite.

STOP RECORDING