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**.

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

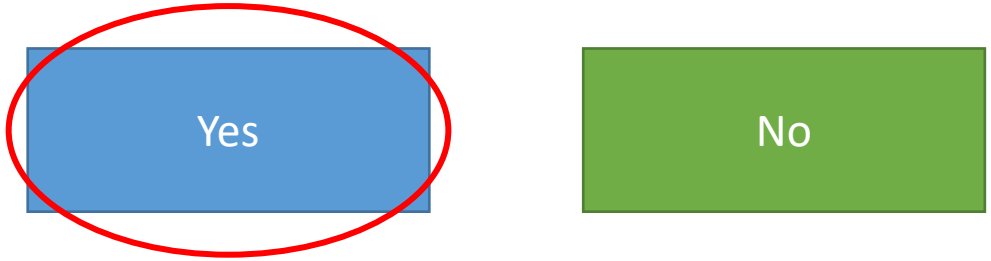
No

Arguing the positive: Universal Statements

- Let's consider the following statement:

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

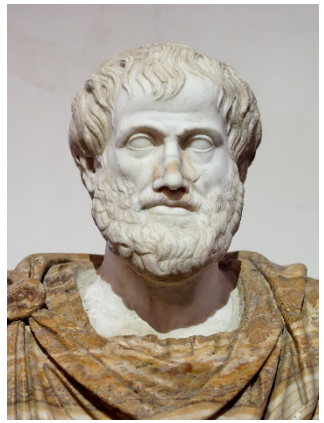
- Do you believe this statement?



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

Proof, verbal style

"Suppose that a is an odd integer and b is an even integer. By the definition of parity, there exist integers c, d such that $a = 2c + 1$ *and* $b = 2d$. *Summing* $a + b$ *yields* $2c + 1 + 2d = 2(c + d) + 1$. *By closure of integers over addition,* $c + d$ *is also an integer, call it* m. *Therefore,* $a + b = 2m + 1$ *and by the definition of parity* $a + b$ *is odd. Done."*



Proof, symbolic style

$$\big((a \text{ is odd}) \wedge (b \text{ is even})\big) \Rightarrow (\exists m, n \in \mathbb{Z})\big[\big((a = 2m + 1) \wedge (b = 2n)\big)\big] \Rightarrow$$
$$(\exists m, n \in \mathbb{Z})[(a + b) = 2\underbrace{(m + n)} + 1 = 2r + 1] \Rightarrow (a + b) \text{ is odd}$$

$r \in \mathbb{Z}$ by closure

Proof, mixed

- Claim to be proven **true** (we argue its **affirmative**):

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

- Proof:
  1. Let n_1 be **any odd integer.** Then, $(\exists k_1 \in \mathbb{Z})[n_1 = 2 \cdot k_1 + 1]$
  2. Let n_2 be **any even integer.** Then, $(\exists k_2 \in \mathbb{Z})[n_2 = 2 \cdot k_2]$
  3. By (1) and (2), we have that $n_1 + n_2 = (2 \cdot k_1 + 1) + 2 \cdot k_2 = 2(k_1 + k_2) + 1$
  4. We set $k_1 + k_2 = r$. By closure of integers over addition, $r \in \mathbb{Z}$.
  5. **Substituting** (4) into (3) yields: $n_1 + n_2 = 2 \cdot r + 1$, which means that $n_1 + n_2$ is odd.
  6. End of proof.

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:** 2

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 tenths and units digits of all perfect squares 16 and above have an absolute difference bigger than 1. Disproof by counterexample: **100**

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 (rare) 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!

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!

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, $(\exists k \in \mathbb{Z})[\, 22r + 18s = 2k]$

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?

Existential statements for you!

- Is there a perfect square 16 or greater whose *units* and *tenths* digits have an absolute difference of 4?

Existential statements for you!

- Is there a perfect square 16 or greater whose *units* and *tenths* digits have an absolute difference of 4?
- $484 = 22^2$

Existential statements for you!

- Is there a perfect square 16 or greater whose *units* and *tenths* digits have an absolute difference of 4?
- $484 = 22^2$
- There is a perfect square 16 or greater whose *units* and *tenths* digits have an absolute difference of 8.

Existential statements for you!

- Is there a perfect square 16 or greater whose *units* and *tenths* digits have an absolute difference of 4?
- $484 = 22^2$
- There is a perfect square 16 or greater whose *units* and *tenths* digits have an absolute difference of 8.
- Let's check a script…

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 $c^{\sqrt{2}} = \left((\sqrt{2})^{\sqrt{2}}\right)^{\sqrt{2}} = (\sqrt{2})^2 = 2 \in \mathbb{Q}$. Since both c and $\sqrt{2}$ are irrationals, but $c^{\sqrt{2}}$ is rational, we are done.

~ negation

Indirect Proofs of Number Theory

1. Manipulate the input.
2. Proceed directly.

- 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 (contrapositive)
  2. Proofs by contradiction
- We will see examples of both.

Proof by contraposition

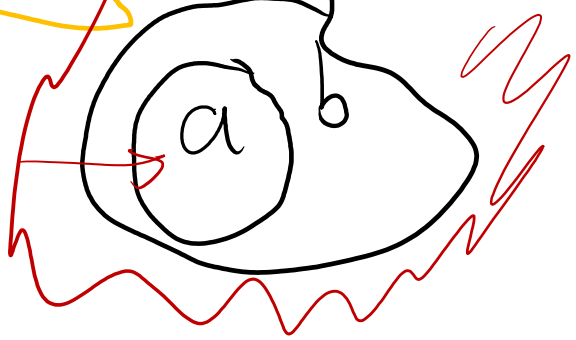
- Applicable to all kinds of statements of type:

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

- 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

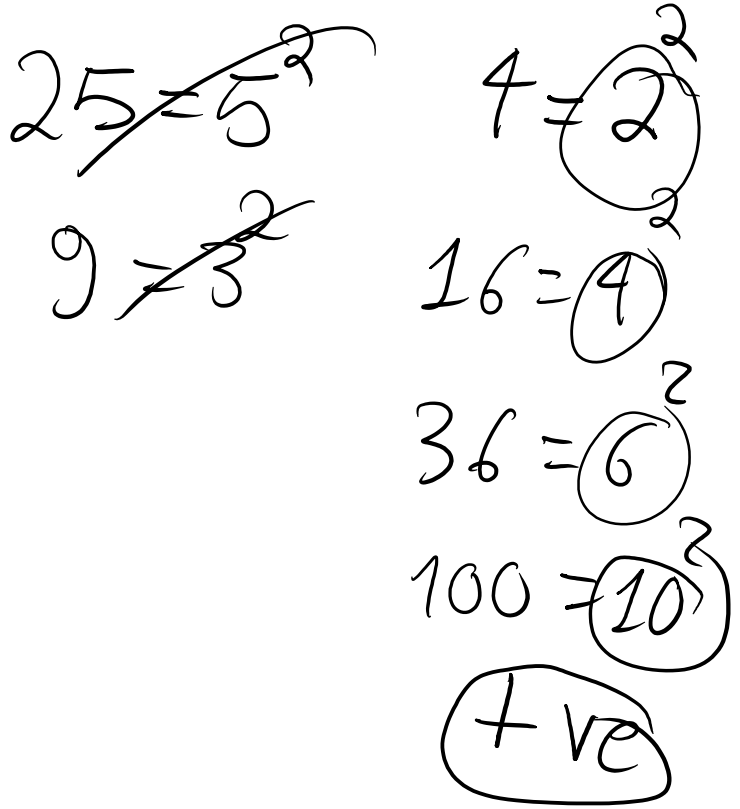
- $(\forall a \in \mathbb{Z})[(a^2\ even) \Rightarrow (a\ even)]$

Examples

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

Yes

No



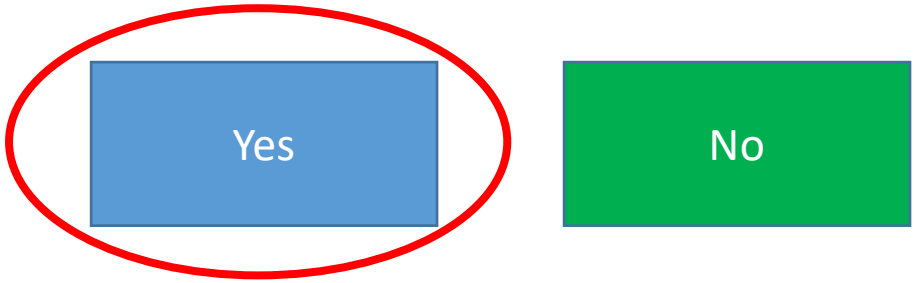
$a^2 \rightarrow a$

Examples

$a^2 = 2k$

$a = \sqrt{2k}$

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



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

Examples

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

First proof we did in this section of proofs!

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

(Listified style, you can choose a different one if you want)

1. Suppose a is an odd integer.
2. By definition of parity, $(\exists k \in \mathbb{Z})[a = 2k + 1]$
3. By algebra, $a^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$
4. Since $\mathbb{Z}$ is closed under both addition and multiplication, $(2k^2 + 2k)$ is an integer. Call this integer r.
5. Substituting the result of (4) into the result of (3) we have: $a^2 = 2r + 1$
6. By the definition of parity, this means that a^2 is odd.
7. End of proof.

$3n+2 = 2r+1$

$n = \frac{2}{3}r - \frac{1}{3}$

Another example

$23 = 3 \cdot 7 + 2$

$17 = 3 \cdot 5 + 2$

$11 = 3 \cdot 3 + 2$

+ve

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

Another example

- Polya's conjecture
- Euler's conjecture 1989

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

$(\forall n \in \mathbb{Z})[(n \text{ is even}) \Rightarrow ((3n+2) \text{ is even})]$

Let's try this one together.

$n = 2k \Rightarrow 3n + 2 = 3(2k) + 2 = 2(3k+1)$

$\leftarrow r \rightarrow$

$= 2r$

Another example

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

$16 = 4 \cdot 4$

$4 \leq \sqrt{16} = 4$

$16 = 1 \cdot 16$

+ve

$16 = 2 \cdot 8$

$2 \leq \sqrt{16} = 4$

Another example

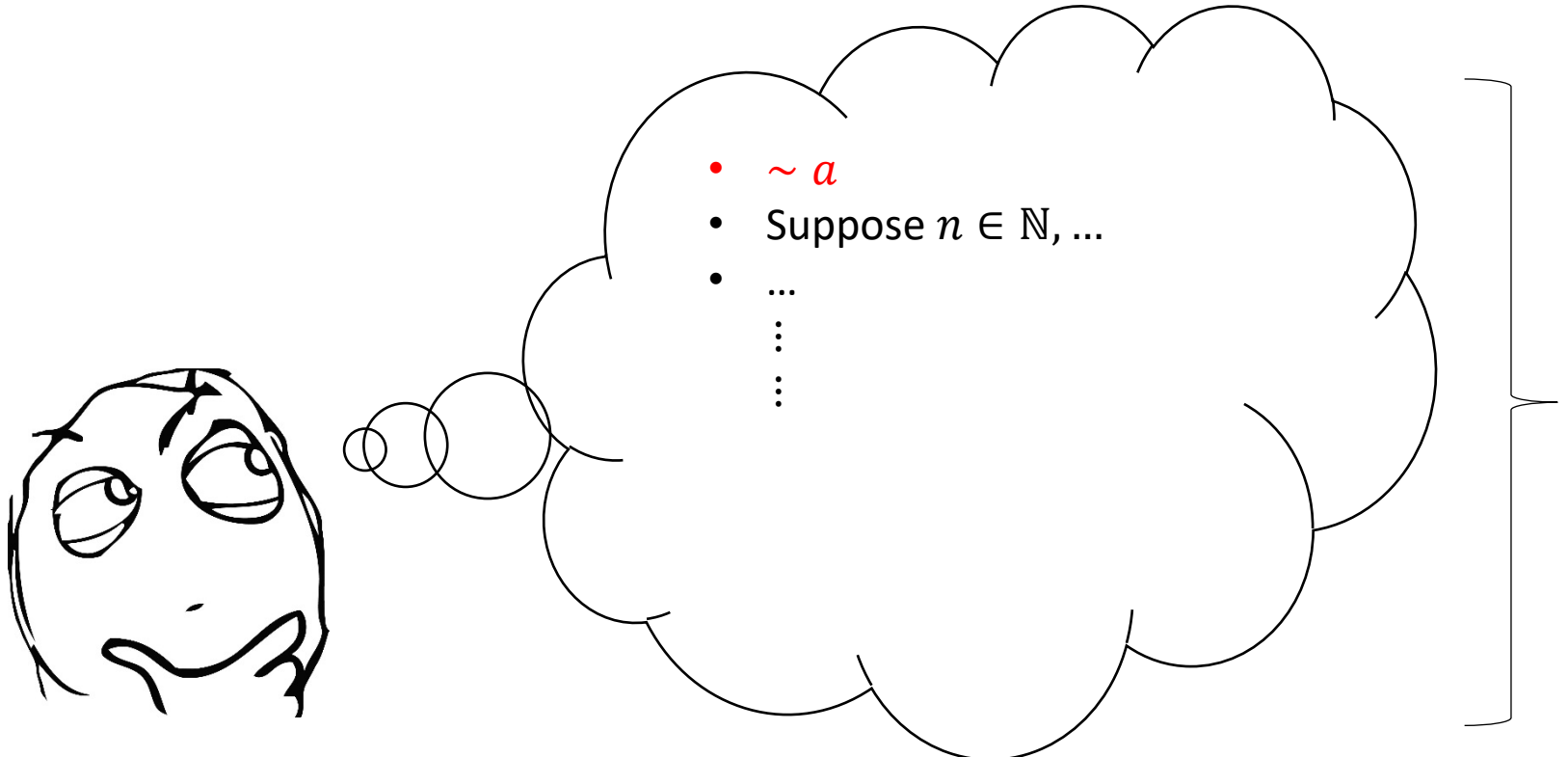
If $n = a \cdot b$, where $a, b \in \mathbb{N}^{\geq 1}$, then $a \leq \sqrt{n}$ OR $b \leq \sqrt{n}$

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 $\sim a$** and **hope that we reach a contradiction** (a falsehood).

Proof by contradiction

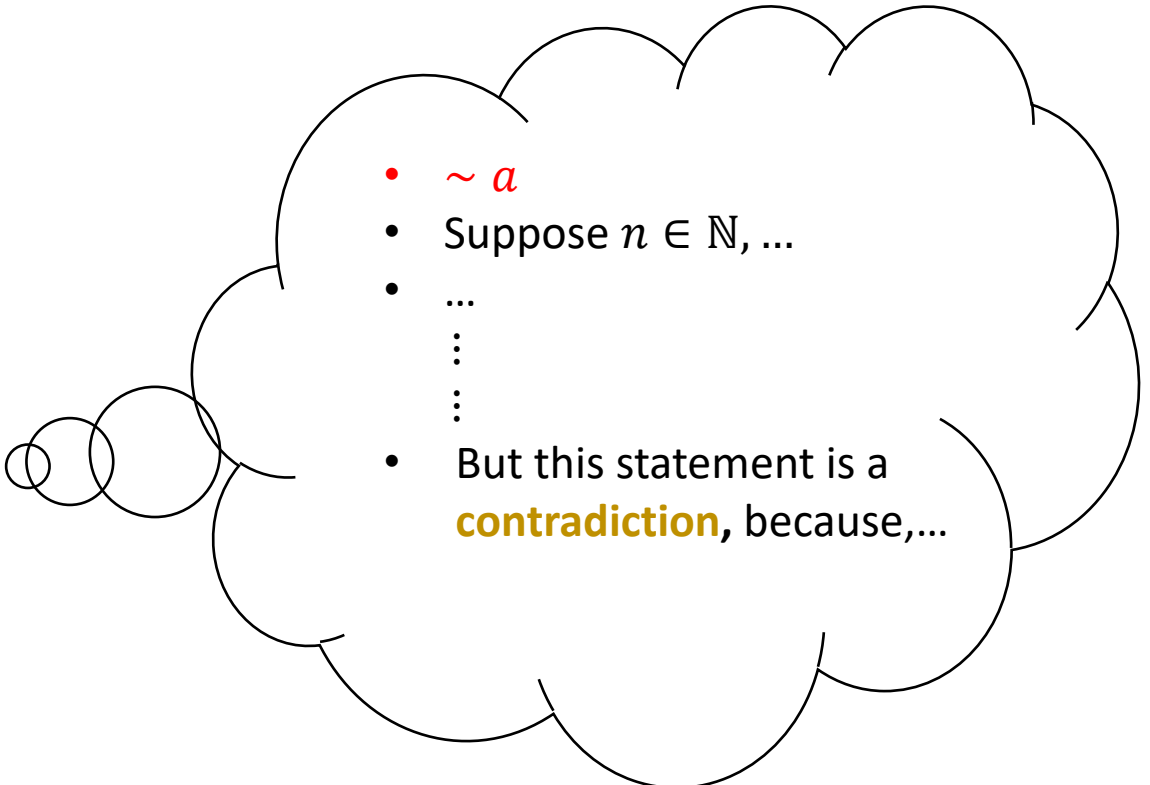
- The most common type of indirect proof is *proof by contradiction*
- Briefly: We want to prove a fact a, so **we assume $\sim a$** and **hope that we reach a contradiction** (a falsehood).



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

Proof by contradiction

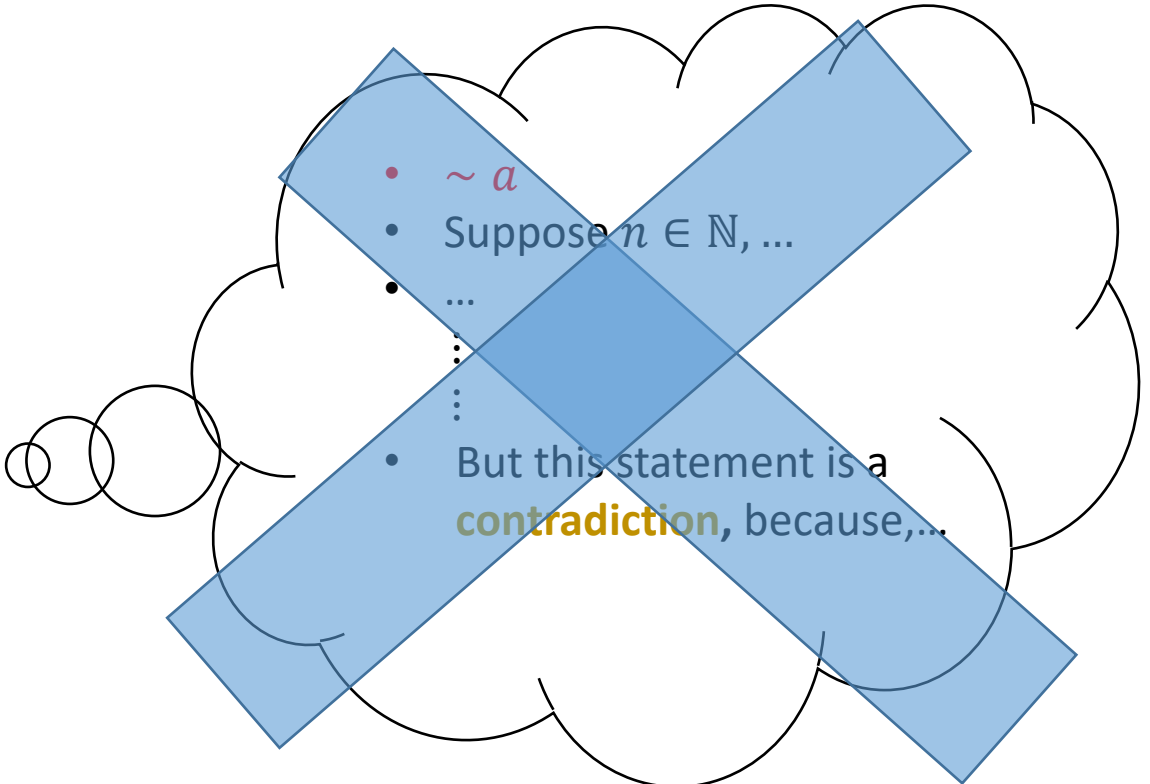
- The most common type of indirect proof is *proof by contradiction*
- Briefly: We want to prove a fact a, so **we assume $\sim a$** and **hope that we reach a contradiction** (a falsehood).



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).

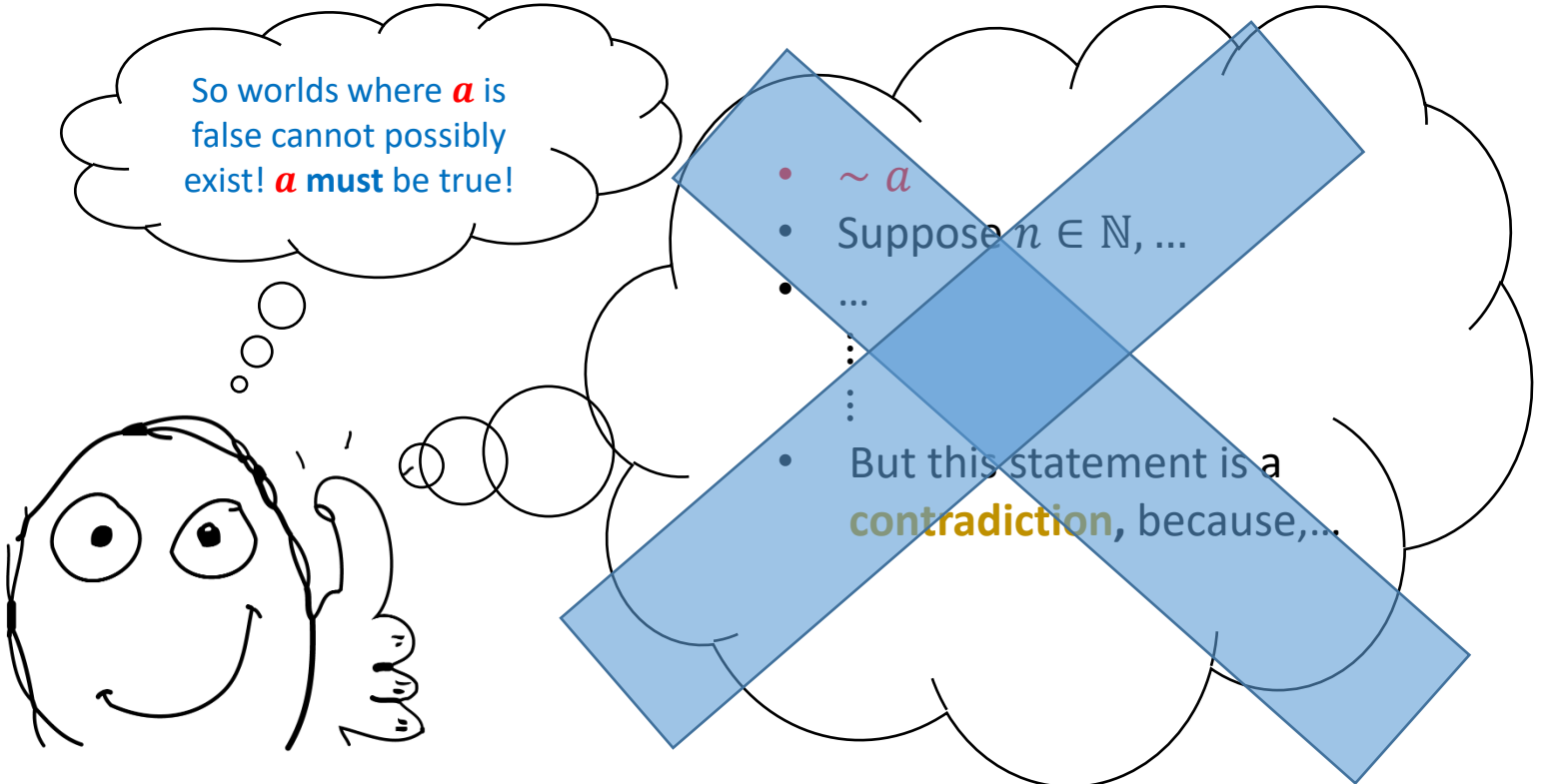


We follow some classic direct proof sets, and reach a statement that is a **logical contradiction!** *(e.g 1 > 2)*

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.

Another

- Statement: There is no least **positive** rational.

Another

- Statement: There is no least **positive** rational.
- Proof (by contradiction):

Another

- Statement: There is no least **positive** rational.
- Proof (by contradiction):
  1. Assume not. Then, there exists a least positive rational.

Another

- Statement: There is no least **positive** rational.
- Proof (by contradiction):
  1. Assume not. Then, there exists a least positive rational.
  2. Let this rational be called q.

Another

- Statement: There is no least **positive** rational.
- Proof (by contradiction):
  1. Assume not. Then, there exists a least positive rational.
  2. Let this rational be called q.
  3. By the definition of rational numbers, $(\exists a, b \in \mathbb{Z}, b \neq 0)[q = \frac{a}{b}]$, where a and b have to have the same sign.

Another

- Statement: There is no least **positive** rational.
- Proof (by contradiction):
  1. Assume not. Then, there exists a least positive rational.
  2. Let this rational be called q.
  3. By the definition of rational numbers, $(\exists a, b \in \mathbb{Z}, b \neq 0)[q = \frac{a}{b}]$, where a and b have to have the same sign.
  4. Regardless of the sign of a and b, $q' = \frac{a}{2 \cdot b}$ is a positive rational, and it also smaller than q.

Another

- Statement: There is no least **positive** rational.
- Proof (by contradiction):
  1. Assume not. Then, there exists a least positive rational.
  2. Let this rational be called q.
  3. By the definition of rational numbers, $(\exists a, b \in \mathbb{Z}, b \neq 0)[q = \frac{a}{b}]$, where a and b have to have the same sign.
  4. Regardless of the sign of a and b, $q' = \frac{a}{2 \cdot b}$ is a positive rational, and it also smaller than q.
  5. Contradiction, since we assumed that q was the least positive rational.

Another

- Statement: There is no least **positive** rational.
- Proof (by contradiction):
  1. Assume not. Then, there exists a least positive rational.
  2. Let this rational be called q.
  3. By the definition of rational numbers, $(\exists a, b \in \mathbb{Z}, b \neq 0)[q = \frac{a}{b}]$, where a and b have to have the same sign.
  4. Regardless of the sign of a and b, $q' = \frac{a}{2 \cdot b}$ is a positive rational, and it also smaller than q.
  5. Contradiction, since we assumed that q was the least positive rational.
  6. Therefore, there does not exist one such least positive rational.

Your turn!

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

Reminders / Your Concerns

- Lifted late homework deadline for homework 7.
  - So submit through tonight for full credit!
- We are aware of 9.4 vs 10 points EC for homework 5, it’s an easy fix.
- Apologies for Gradescope not allowing partial credit for multiple questions.
- When we end mods (today / Thursday) we are done with M2 material.

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, there exists a unique integer q such that a can be written in one of 4 ways:

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, there exists a unique integer q such that a can be written in one of 4 ways:

   a) $(a = 5q + 1) \Rightarrow a^2 = 25q^2 + 10q + 1 = 5\underbrace{(5q^2 + 2q)}_{m \in \mathbb{Z}} + 1 = 5m + 1 \Rightarrow a^2$ not 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, there exists a unique integer q such that a can be written in one of 4 ways:

a) $(a = 5q + 1) \Rightarrow a^2 = 25q^2 + 10q + 1 = 5\underbrace{(5q^2 + 2q)}_{m \in \mathbb{Z}} + 1 = 5m + 1 \Rightarrow a^2$ not multiple of 5

b) $(a = 5q + 2) \Rightarrow a^2 = 25q^2 + 20q + 4 = 5(5q^2 + 4q) + 4 = 5m + 4 \Rightarrow a^2$ not 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, there exists a unique integer q such that a can be written in one of 4 ways:

a) $(a = 5q + 1) \Rightarrow a^2 = 25q^2 + 10q + 1 = 5\underbrace{(5q^2 + 2q)}_{m \in \mathbb{Z}} + 1 = 5m + 1 \Rightarrow a^2$ not multiple of 5

b) $(a = 5q + 2) \Rightarrow a^2 = 25q^2 + 20q + 4 = 5(5q^2 + 4q) + 4 = 5m + 4 \Rightarrow a^2$ not multiple of 5

c) $(a = 5q + 3) \Rightarrow a^2 = 25q^2 + 30q + \underbrace{9}_{5+4} = 5(5q^2 + 6q + 1) + 4 = 5m + 4 \Rightarrow a^2$ not 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, there exists a unique integer q such that a can be written in one of 4 ways:

a) $(a = 5q + 1) \Rightarrow a^2 = 25q^2 + 10q + 1 = 5\underbrace{(5q^2 + 2q)}_{m \in \mathbb{Z}} + 1 = 5m + 1 \Rightarrow a^2$ not multiple of 5

b) $(a = 5q + 2) \Rightarrow a^2 = 25q^2 + 20q + 4 = 5(5q^2 + 4q) + 4 = 5m + 4 \Rightarrow a^2$ not multiple of 5

c) $(a = 5q + 3) \Rightarrow a^2 = 25q^2 + 30q + \underbrace{9}_{5+4} = 5(5q^2 + 6q + 1) + 4 = 5m + 4 \Rightarrow a^2$ not multiple of 5

d) $(a = 5q + 4) \Rightarrow a^2 = 25q^2 + 40q + \underbrace{16}_{3*5+1} = 5(5q^2 + 8q + 3) + 1 = 5m + 1 \Rightarrow a^2$ not 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, there exists a unique integer q such that a can be written in one of 4 ways:

a) $(a = 5q + 1) \Rightarrow a^2 = 25q^2 + 10q + 1 = 5\underbrace{(5q^2 + 2q)}_{m \in \mathbb{Z}} + 1 = 5m + 1 \Rightarrow a^2$ not multiple of 5

b) $(a = 5q + 2) \Rightarrow a^2 = 25q^2 + 20q + 4 = 5(5q^2 + 4q) + 4 = 5m + 4 \Rightarrow a^2$ not multiple of 5

c) $(a = 5q + 3) \Rightarrow a^2 = 25q^2 + 30q + \underbrace{9}_{5+4} = 5(5q^2 + 6q + 1) + 4 = 5m + 4 \Rightarrow a^2$ not multiple of 5

d) $(a = 5q + 4) \Rightarrow a^2 = 25q^2 + 40q + \underbrace{16}_{3*5+1} = 5(5q^2 + 8q + 3) + 1 = 5m + 1 \Rightarrow a^2$ not multiple of 5

3. So, in all possible cases, we found that a^2 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, there exists a unique integer q such that a can be written in one of 4 ways:

a) $(a = 5q + 1) \Rightarrow a^2 = 25q^2 + 10q + 1 = 5\underbrace{(5q^2 + 2q)}_{m \in \mathbb{Z}} + 1 = 5m + 1 \Rightarrow a^2$ not multiple of 5

b) $(a = 5q + 2) \Rightarrow a^2 = 25q^2 + 20q + 4 = 5(5q^2 + 4q) + 4 = 5m + 4 \Rightarrow a^2$ not multiple of 5

c) $(a = 5q + 3) \Rightarrow a^2 = 25q^2 + 30q + \underbrace{9}_{5+4} = 5(5q^2 + 6q + 1) + 4 = 5m + 4 \Rightarrow a^2$ not multiple of 5

d) $(a = 5q + 4) \Rightarrow a^2 = 25q^2 + 40q + \underbrace{16}_{3*5+1} = 5(5q^2 + 8q + 3) + 1 = 5m + 1 \Rightarrow a^2$ not multiple of 5

3. So, in all possible cases, we found that a^2 is not a multiple of 5.
4. Done.

Proof of lemma

- Proof (by contraposition): We prove that:

1.
2. ays:
   ple of 5
   le of 5
   ultiple of 5
   multiple of 5
3. So, in all possible cases, we found that a^2 is not a multiple of 5.
4. Done.

CAN WE MAKE THIS A BIT SHORTER? What if instead of 5 we had 101? Would we do 100 cases?

Proof of lemma

- Proof (by contraposition): We prove that:

1.
2. ays:
   ple of 5
   le of 5
   ultiple of 5
   multiple of 5
3. So, in all possible cases, we found that a^2 is not a multiple of 5.
4. Done.

CAN WE MAKE THIS A BIT SHORTER? What if instead of 5 we had 101? Would we do 100 cases?

(Let's solve this later…)

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

You may assume that the lemma

a^2 is mult. 7 => a is mult. 7

has been proven to be **true.**

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

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

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 $p_1, p_2, \ldots, p_k$ like so:

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

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 (and we will do it)
- Proving uniqueness is harder (and maybe we ask it in an exam)

Examples of “uniqueness”

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

Time to solve our lemma problem!

- Proof (by contraposition): We prove that:

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

1.
2. ays:
   ple of 5
   le of 5
   ultiple of 5
   multiple of 5
3.
4. Done.

What if 5 were 101? How can we avoid 100 different cases?

Time to solve our lemma problem!

- Proof (by contraposition): We prove that:

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

- Suppose that the UPF of a is $p_1^{e_1} \cdot p_2^{e_2} \cdot \dots p_k^{e_k}$
- Since a is **not** a multiple of 5, and 5 is prime, 5 is **not** one of those p_i!
- Then, UPF of a^2 is $p_1^{2e_1} \cdot p_2^{2e_2} \cdot \dots p_k^{2e_k}$
- We already know that 5 is **not** one of those p_i, so it's also **not** in the UPFT of a^2!
- So 5 does **not** divide a^2!

Another necessary lemma

Set of primes

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

Another 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.