START RECORDING

Techniques of proof

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

Direct Proofs

Basic definitions: Parity

- n is even iff $n \equiv \; 0 \pmod{2}$

- n is odd iff $n \equiv 1 \pmod{2}$

- If $n \equiv b \pmod{2}$ where $b \in \{0,1\}$ then b is the parity of n.

Statements of claims / theorems

- The sum of an even and an odd is odd

Statements of claims / theorems

- The sum of an even and an odd is odd
  - x even, so $x \equiv 0 \pmod 2$
  - y odd, so $y \equiv 1 \pmod 2$
    - $x + y \equiv 0 + 1 \equiv 1 \pmod 2$.

Statements of claims / theorems

- The sum of an even and an odd is odd
  - x even, so $x \equiv 0 \pmod{2}$
  - y odd, so $y \equiv 1 \pmod{2}$
    - $x + y \equiv 0 + 1 \equiv 0 \pmod{2}$.

- If a is an integer, then $a^2 + a$ is even.

Statements of claims / theorems

- The sum of an even and an odd is odd
  - x even, so $x \equiv 0 \pmod 2$
  - y odd, so $y \equiv 1 \pmod 2$
    - $x + y \equiv 0 + 1 \equiv 0 \pmod 2$.

- If a is an integer, then $a^2 + a$ is even.
  - a even, so $a \equiv 0 \pmod 2$
    - $0^2 + 0 \equiv 0 \pmod 2$
  - a odd, so $a \equiv 1 \pmod 2$
    - $1^2 + 1 \equiv 0 \pmod 2$

Statements of claims / theorems

- If $x \equiv 1 \pmod 3$ and $y \equiv 2 \pmod 3$ then $x + y \equiv 0 \pmod 3$.

Statements of claims / theorems

- If $x \equiv 1 \pmod 3$ and $y \equiv 2 \pmod 3$ then $x + y \equiv 0 \pmod 3$.

- For all x, $x^2 \equiv 0$ or 1 or $4 \pmod 8$
  - (We will use this later.)

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

Proof By Contrapostition

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

- $(\forall a \in \mathbb{Z})\left[\left(a^2 \equiv 0 \pmod{2}\right) \Rightarrow \left(a \equiv 0 \pmod{2}\right)\right]$

Examples

- $(\forall a \in \mathbb{Z})\left[\left(a^2 \equiv 0 \pmod{2}\right) \Rightarrow \left(a \equiv 0 \pmod{2}\right)\right]$
- Do we believe this to be true?

Yes

No

Examples

- $(\forall a \in \mathbb{Z})\left[\left(a^2 \equiv 0 \pmod 2\right) \Rightarrow \left(a \equiv 0 \pmod 2\right)\right]$
- Do we believe this to be true?

Yes

No

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

Examples

- $(\forall a \in \mathbb{Z})\left[\left(a^2 \equiv 0 \pmod 2\right) \Rightarrow \left(a \equiv 0 \pmod 2\right)\right]$
- Proving this ***directly*** is somewhat hard
- On the other hand, the **contrapositive**

$$(\forall a \in \mathbb{Z})[\ (a \equiv 1 \pmod 2) \Rightarrow (a^2 \equiv 1 \pmod 2)]$$

is **much easier**!

Proof that $(\forall a \in \mathbb{Z})[\left(a \equiv 1\ (mod\ 2)\right) \Rightarrow (a^2 \equiv 1\ (\mathrm{mod}\ 2))]$

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.

Proof that $(\forall a \in \mathbb{Z})[\left(a^2 \equiv 0\ (mod\ 3)\right) \Rightarrow (a \equiv 0 \pmod 3)]$

1. Contrapositive $\left(a \not\equiv 0\ (mod\ 3)\right) \Rightarrow$
   $(a^2 \not\equiv 0 \pmod 3)$

Proof that $(\forall a \in \mathbb{Z})\left[\left(a^2 \equiv 0\ (mod\ 3)\right) \Rightarrow (a \equiv 0\ (\text{mod}\ 3))\right]$

1. Contrapositive $\left(a \not\equiv 0\ (mod\ 3)\right) \Rightarrow$
$$(a^2 \not\equiv 0\ (\text{mod}\ 3))$$
2. Case 1 $a \equiv 1\ (mod\ 3)$
   1. $a^2 \equiv 1^2 \equiv 1\ (mod\ 3)$

Proof that $(\forall a \in \mathbb{Z})[\left(a^2 \equiv 0\ (mod\ 3)\right) \Rightarrow (a \equiv 0\ (\mathrm{mod}\ 3))]$

1. Contrapositive $\left(a \not\equiv 0\ (mod\ 3)\right) \Rightarrow$ $(a^2 \not\equiv 0\ (\mathrm{mod}\ 3))$
2. Case 1 $a \equiv 1\ (mod\ 3)$
   1. $a^2 \equiv 1^2 \equiv 1\ (mod\ 3)$
3. Case 2 $a \equiv 2\ (mod\ 3)$
   1. $a^2 \equiv 2^2 \equiv 1\ (mod\ 3)$

Proof that $(\forall a \in \mathbb{Z})[\left(a^2 \equiv 0\ (mod\ 3)\right) \Rightarrow (a \equiv 0 \pmod 3)]$

1. Contrapositive $\left(a \not\equiv 0\ (mod\ 3)\right) \Rightarrow (a^2 \not\equiv 0 \pmod 3)$
2. Case 1 $a \equiv 1\ (mod\ 3)$
   1. $a^2 \equiv 1^2 \equiv 1\ (mod\ 3)$
3. Case 2 $a \equiv 2\ (mod\ 3)$
   1. $a^2 \equiv 2^2 \equiv 1\ (mod\ 3)$
4. Done.

Is $(\forall a \in \mathbb{Z})[\left(a^2 \equiv 0\ (mod\ 4)\right) \Rightarrow (a \equiv 0 \pmod 4)]$ true?

Is $(\forall a \in \mathbb{Z})[\left(a^2 \equiv 0\ (mod\ 4)\right) \Rightarrow (a \equiv 0\ (\mathrm{mod}\ 4))]$ true?

Proof?

1. Contrapositive $\left(a \not\equiv 0\ (mod\ 4)\right) \Rightarrow \left(a^2 \not\equiv 0\ (mod\ 4)\right)$
2. Case 1 $a \equiv 1\ (mod\ 4)$
   1. $a^2 \equiv 1^2 \equiv 1\ (mod\ 4)$
3. Case 2 $a \equiv 2\ (mod\ 4)$
   1. $a^2 \equiv 2^2 \equiv 0\ (mod\ 4)$
4. Fails when $a \equiv 2\ (mod\ 4)$

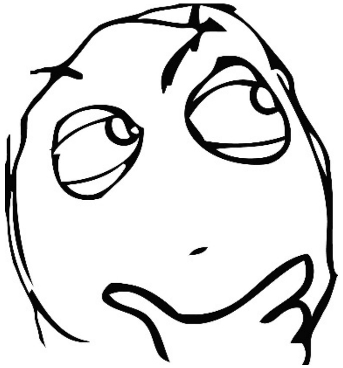
Proof by Contradiction

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



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

$\vdots$

$\vdots$

This is a so-called **“conditional world”** It’s a “version” of our world **where we assume $\sim \boldsymbol{a}$.**

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

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

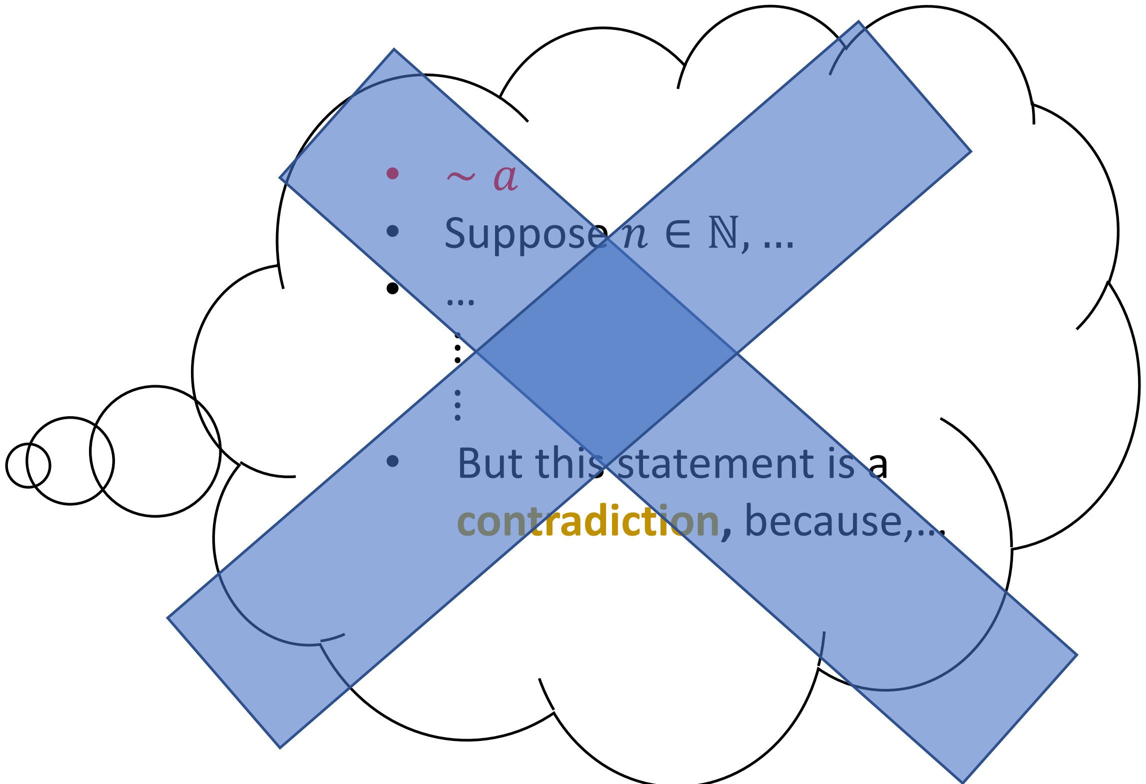
  ⋮

  ⋮
- 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).

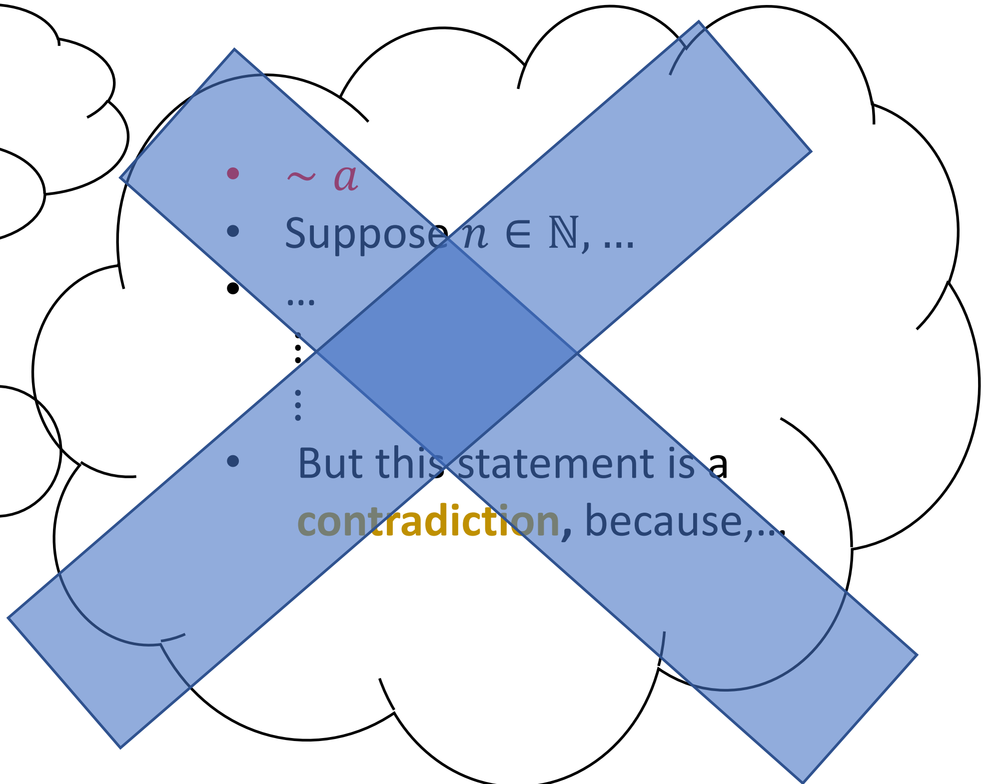


We follow some classic direct proof sets, and reach a statement that is a **logical contradiction!** *(e.g 1 > 2)*

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 $a \equiv 0 \pmod{2}$ **(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 $a \equiv 0 \pmod 2$ **(2)**
6. Substituting **(2)** into **(1)** yields $0^2 \pmod 2 \equiv 2b^2 \Rightarrow b^2 \equiv 0 \pmod 2 \Rightarrow$

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 $a \equiv 0 \pmod 2$ **(2)**
6. Substituting **(2)** into **(1)** yields $0^2 \pmod 2 \equiv 2b^2 \Rightarrow b^2 \equiv 0 \pmod 2 \Rightarrow$
7. $b^2 \equiv 0 \pmod 2 \Rightarrow$ 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 $a \equiv 0 \pmod 2$ **(2)**
6. Substituting **(2)** into **(1)** yields $0^2 \pmod 2 \equiv 2b^2 \Rightarrow b^2 \equiv 0 \pmod 2 \Rightarrow$
7. $b^2 \equiv 0 \pmod 2 \Rightarrow$ 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 $a \equiv 0 \pmod 2$ **(2)**
6. Substituting **(2)** into **(1)** yields $0^2 (\text{mod } 2) \equiv 2b^2 \Rightarrow b^2 \equiv 0 \pmod 2 \Rightarrow$
7. $b^2 \equiv 0 \pmod 2 \Rightarrow b$ 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

$$\text{If } a^2 \text{ is a multiple of 5, then so is } a$$

$$\Leftrightarrow$$

$$\text{If } a \text{ is not a multiple of 5, then } a^2 \text{ isn't one either.}$$

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)**

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 $a \equiv 0 \pmod 5$ **(2)**

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 $a \equiv 0 \pmod 5$ **(2)**
- Substituting (2) into (1) yields $0^2 (\bmod 5) \equiv 5b^2 \Rightarrow b^2 \equiv 0 \pmod 5 \Rightarrow$

  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 $x = 2$

Enroute to an alternative proof that numbers are irrational

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 (Formally needs induction which we will do later in this course)

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 (Formally needs induction which we will do later in this course)
- 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, $p \nmid (a+1)$.

STOP

RECORDING