## About definitions and quiz

**Definition.**

**Verbally.** Let $p > 1$ be an integer.
$p$ is called **prime**
if it has only two positive divisors: $1$ and $p$.

**Symbolically.** Let $p \in \mathbb{Z}$ and $p > 1$.
$p$ is **prime** $\iff \forall k \in \mathbb{Z}_+ \ (k \mid p \implies k = 1 \vee k = p)$.

Let $n > 1$ be an integer.
$n$ is called **composite**
if it has more than two positive divisors.

# About definitions and quiz

**Definition.** Let ______________________________.
**description of universes, objects, variables**

**Verbally.** Let $p > 1$ be an integer.
$p$ is called **prime**
if it has only two positive divisors: $1$ and $p$.

**Symbolically.** Let $p \in \mathbb{Z}$ and $p > 1$.
$p$ is **prime** $\iff \forall k \in \mathbb{Z}_+ \ (k \mid p \implies k = 1 \vee k = p)$.

Let $n > 1$ be an integer.
$n$ is called **composite**
if it has more than two positive divisors.

# About definitions and quiz

**Definition.** Let ______________________________.
**description of universes, objects, variables**

____________ is called / is said to be / is __________________
**object**

**Verbally.** Let $p > 1$ be an integer.
$p$ is called **prime**
if it has only two positive divisors: $1$ and $p$.

**Symbolically.** Let $p \in \mathbb{Z}$ and $p > 1$.
$p$ is **prime** $\iff \forall k \in \mathbb{Z}_+ \ (k \mid p \implies k = 1 \lor k = p)$.

Let $n > 1$ be an integer.
$n$ is called **composite**
if it has more than two positive divisors.

# About definitions and quiz

**Definition.** Let ______________________________.
**description of universes, objects, variables**

______________ is called / is said to be / is ______________________
**object** **term**

**Verbally.** Let $p > 1$ be an integer.
$p$ is called **prime**
if it has only two positive divisors: $1$ and $p$.

**Symbolically.** Let $p \in \mathbb{Z}$ and $p > 1$.
$p$ is **prime** $\iff \forall k \in \mathbb{Z}_+ \ (k \mid p \implies k = 1 \vee k = p)$.

Let $n > 1$ be an integer.
$n$ is called **composite**
if it has more than two positive divisors.

# About definitions and quiz

**Definition.** Let ________________________________________.

**description of universes, objects, variables**

________________ is called / is said to be / is ________________________________

**object** **term**

if

**Verbally.** Let $p > 1$ be an integer.
$p$ is called **prime**
if it has only two positive divisors: $1$ and $p$.

**Symbolically.** Let $p \in \mathbb{Z}$ and $p > 1$.
$p$ is **prime** $\iff \forall k \in \mathbb{Z}_+ \ (k \mid p \implies k = 1 \vee k = p)$.

Let $n > 1$ be an integer.
$n$ is called **composite**
if it has more than two positive divisors.

# About definitions and quiz



**Definition.** Let ________________________________.
description of universes, objects, variables

____________ is called / is said to be / is ____________________
object — term

if ← if always means iff in definitions

**Verbally.** Let $p > 1$ be an integer.

$p$ is called **prime**

if it has only two positive divisors: $1$ and $p$.

**Symbolically.** Let $p \in \mathbb{Z}$ and $p > 1$.

$p$ is **prime** $\iff \forall k \in \mathbb{Z}_+ \ (k \mid p \implies k = 1 \vee k = p)$.

Let $n > 1$ be an integer.

$n$ is called **composite**

if it has more than two positive divisors.

# About definitions and quiz



**Definition.** Let ______________________________________.
**description of universes, objects, variables**

_______________ is called / is said to be / is ________________________
**object** **term**

if ← **if always means iff in definitions**

__________________________________________________.
**distinguishing characteristic**

# About definitions and quiz



**Definition.** Let ______________________________.
**description of universes, objects, variables**

______________ is called / is said to be / is ______________________
**object** **term**

if ← **if <u>always</u> means iff in definitions**

______________________________________________.
**distinguishing characteristic**

**Verbally.** Let $p > 1$ be an integer.

# About definitions and quiz

**Definition.** Let ________________________.
**description of universes, objects, variables**

__________ (**object**) is called / is said to be / is ____________ (**term**)

if ← **if always means iff in definitions**

________________________.
**distinguishing characteristic**

**Verbally.** Let $p > 1$ be an integer.

$p$

# About definitions and quiz

**Definition.** Let ________________________________.
**description of universes, objects, variables**

____________ is called / is said to be / is ____________________
**object** **term**

if ← **if always means iff in definitions**

______________________________________.
**distinguishing characteristic**

**Verbally.** Let $p > 1$ be an integer.
$p$ is called

# About definitions and quiz

**Definition.** Let ________________________________.
**description of universes, objects, variables**

____________ is called / is said to be / is ____________________
**object** **term**

if ← **if always means iff in definitions**

________________________________________.
**distinguishing characteristic**

**Verbally.** Let $p > 1$ be an integer.
$p$ is called **prime**

# About definitions and quiz

**Definition.** Let ______________________________.
**description of universes, objects, variables**

______________ is called / is said to be / is ______________________
**object** **term**

if ← **if always means iff in definitions**

________________________________________.
**distinguishing characteristic**

**Verbally.** Let $p > 1$ be an integer.
$p$ is called **prime**
if it has only two positive divisors: $1$ and $p$.

# About definitions and quiz

**Definition.** Let ____________________.
description of universes, objects, variables

__________ (object) is called / is said to be / is __________ (term)

if ← if always means iff in definitions

____________________.
distinguishing characteristic

**Verbally.** Let $p > 1$ be an integer.

$p$ is called **prime**

if it has only two positive divisors: $1$ and $p$.

**Symbolically.** Let $p \in \mathbb{Z}$ and $p > 1$.

# About definitions and quiz

**Definition.** Let ____________________.
**description of universes, objects, variables**

__________ is called / is said to be / is _______________
**object** **term**

if ← **if always means iff in definitions**

______________________________.
**distinguishing characteristic**

**Verbally.** Let $p > 1$ be an integer.
$p$ is called **prime**
if it has only two positive divisors: $1$ and $p$.

**Symbolically.** Let $p \in \mathbb{Z}$ and $p > 1$.
$p$ is **prime**

# About definitions and quiz

**Definition.** Let ________________________________.
**description of universes, objects, variables**

____________ (**object**) is called / is said to be / is ________________ (**term**)

if ← **if always means iff in definitions**

________________________________________.
**distinguishing characteristic**

**Verbally.** Let $p > 1$ be an integer.
$p$ is called **prime**
if it has only two positive divisors: $1$ and $p$.

**Symbolically.** Let $p \in \mathbb{Z}$ and $p > 1$.
$p$ is **prime** $\iff \forall k \in \mathbb{Z}_+ \ (k \mid p \implies k = 1 \lor k = p)$.

# About definitions and quiz

**Definition.** Let ______________________________.
description of universes, objects, variables

______________ is called / is said to be / is ______________
object — term

if ← if always means iff in definitions

______________________________.
distinguishing characteristic

**Verbally.** Let $p > 1$ be an integer.
$p$ is called **prime**
if it has only two positive divisors: $1$ and $p$.

**Symbolically.** Let $p \in \mathbb{Z}$ and $p > 1$.
$p$ is **prime** $\iff \forall k \in \mathbb{Z}_+ \ (k \mid p \implies k = 1 \vee k = p)$.

Let $n > 1$ be an integer.
$n$ is called **composite**

# About definitions and quiz

**Definition.** Let ____________________________.
**description of universes, objects, variables**

____________ is called / is said to be / is __________________
**object** **term**

if ← **if always means iff in definitions**

__________________________________.
**distinguishing characteristic**

**Verbally.** Let $p > 1$ be an integer.
$p$ is called **prime**
if it has only two positive divisors: $1$ and $p$.

**Symbolically.** Let $p \in \mathbb{Z}$ and $p > 1$.
$p$ is **prime** $\iff \forall k \in \mathbb{Z}_+ \ (k \mid p \implies k = 1 \vee k = p)$.

Let $n > 1$ be an integer.
$n$ is called **composite**
if it has more than two positive divisors.

# Mistakes in a definition

# Mistakes in a definition



An integer with exactly two divisors is $-1$ !

# Mistakes in a definition



An integer with exactly two divisors is $-1$ !

Missing or wrong universe.

# Mistakes in a definition

An integer with exactly two divisors is $-1$ !

Missing or wrong universe.

Object of definition under quantifier.

# Mistakes in a definition

An integer with exactly two divisors is $-1$ !

Missing or wrong universe.

Object of definition under quantifier.(It must be free!)

# Mistakes in a definition

An integer with exactly two divisors is $-1$ !

Missing or wrong universe.

Object of definition under quantifier.(It must be free!)

A free variable which is not object of definition.

# Mistakes in a definition

An integer with exactly two divisors is $-1$!

Missing or wrong universe.

Object of definition under quantifier.(It must be free!)

A free variable which is not object of definition.

Hinting (implicit) notation.

# Mistakes in a definition

An integer with exactly two divisors is $-1$ !

Missing or wrong universe.

Object of definition under quantifier.(It must be free!)

A free variable which is not object of definition.

Hinting (implicit) notation. E.g., $d$ does not mean **divisor**

# Mistakes in a definition

An integer with exactly two divisors is $-1$ !

Missing or wrong universe.

Object of definition under quantifier.(It must be free!)

A free variable which is not object of definition.

Hinting (implicit) notation. E.g., $d$ does not mean **divisor**

Confusion in symbols of logical connectives.

## Mistakes in a definition



An integer with exactly two divisors is $-1$!

Missing or wrong universe.

Object of definition under quantifier.(It must be free!)

A free variable which is not object of definition.

Hinting (implicit) notation. E.g., $d$ does not mean **divisor**

Confusion in symbols of logical connectives.

# Proof by contradiction (indirect proof)



Idea: To prove $P$,

# Proof by contradiction (indirect proof)



Idea: To prove $P$, we assume $\neg P$

# Proof by contradiction (indirect proof)



Idea: To prove $P$, we assume $\neg P$ and get two mutually exclusive statements,

# Proof by contradiction (indirect proof)



Idea: To prove $P$, we assume $\neg P$ and get two mutually exclusive statements, $Q$ and $\neg Q$.

# Proof by contradiction (indirect proof)



Idea: To prove $P$, we assume $\neg P$ and get two mutually exclusive statements, $Q$ and $\neg Q$.

Logical justification: $(\neg P \implies Q) \wedge (\neg P \implies \neg Q)) \implies P$ is a tautology.

# Proof by contradiction (indirect proof)



Idea: To prove $P$, we assume $\neg P$ and get two mutually exclusive statements, $Q$ and $\neg Q$.

Logical justification: $(\neg P \implies Q) \wedge (\neg P \implies \neg Q)) \implies P$ is a tautology.

This rule of logical deduction is called **reductio ad absurdum**.

# Proof by contradiction (indirect proof)



Idea: To prove $P$, we assume $\neg P$ and get two mutually exclusive statements, $Q$ and $\neg Q$.

Logical justification: $(\neg P \implies Q) \wedge (\neg P \implies \neg Q)) \implies P$ is a tautology.

This rule of logical deduction is called **reductio ad absurdum**.

It is based on the **law of excluded middle**: $P \vee \neg P$ is a tautology.

# Proof by contradiction (indirect proof)

Idea: To prove $P$, we assume $\neg P$ and get two mutually exclusive statements, $Q$ and $\neg Q$.

Logical justification: $(\neg P \implies Q) \wedge (\neg P \implies \neg Q)) \implies P$ is a tautology.

This rule of logical deduction is called **reductio ad absurdum**.

It is based on the **law of excluded middle**: $P \vee \neg P$ is a tautology.

Method: Assume (let) $\neg P$.

# Proof by contradiction (indirect proof)



Idea: To prove $P$, we assume $\neg P$ and get two mutually exclusive statements, $Q$ and $\neg Q$.

Logical justification: $(\neg P \implies Q) \wedge (\neg P \implies \neg Q)) \implies P$ is a tautology.

This rule of logical deduction is called **reductio ad absurdum**.

It is based on the **law of excluded middle**: $P \vee \neg P$ is a tautology.

Method: Assume (let) $\neg P$. Then ... $Q$.

# Proof by contradiction (indirect proof)

Idea: To prove $P$, we assume $\neg P$ and get two mutually exclusive statements, $Q$ and $\neg Q$.

Logical justification: $(\neg P \implies Q) \wedge (\neg P \implies \neg Q)) \implies P$ is a tautology.

This rule of logical deduction is called **reductio ad absurdum**.

It is based on the **law of excluded middle**: $P \vee \neg P$ is a tautology.

Method: Assume (let) $\neg P$. Then ... $Q$. Then ... $\neg Q$.

# Proof by contradiction (indirect proof)



Idea: To prove $P$, we assume $\neg P$ and get two mutually exclusive statements, $Q$ and $\neg Q$.

Logical justification: $(\neg P \implies Q) \wedge (\neg P \implies \neg Q)) \implies P$ is a tautology.

This rule of logical deduction is called **reductio ad absurdum**.

It is based on the **law of excluded middle**: $P \vee \neg P$ is a tautology.

Method: Assume (let) $\neg P$. Then ... $Q$. Then ... $\neg Q$. Therefore, $P$.

# Proof by contradiction (indirect proof)

Idea: To prove $P$, we assume $\neg P$ and get two mutually exclusive statements, $Q$ and $\neg Q$.

Logical justification: $(\neg P \implies Q) \wedge (\neg P \implies \neg Q)) \implies P$ is a tautology.

This rule of logical deduction is called **reductio ad absurdum**.

It is based on the **law of excluded middle**: $P \vee \neg P$ is a tautology.

Method: Assume (let) $\neg P$. Then ... $Q$. Then ... $\neg Q$. Therefore, $P$.

**Example 1.**

# Proof by contradiction (indirect proof)



Idea: To prove $P$, we assume $\neg P$ and get two mutually exclusive statements, $Q$ and $\neg Q$.

Logical justification: $(\neg P \implies Q) \wedge (\neg P \implies \neg Q)) \implies P$ is a tautology.

This rule of logical deduction is called **reductio ad absurdum**.

It is based on the **law of excluded middle**: $P \vee \neg P$ is a tautology.

Method: Assume (let) $\neg P$. Then ... $Q$. Then ... $\neg Q$. Therefore, $P$.

**Example 1.** Prove that $\sqrt{2}$ is irrational.

# Proof by contradiction (indirect proof)

Idea: To prove $P$, we assume $\neg P$ and get two mutually exclusive statements, $Q$ and $\neg Q$.

Logical justification: $(\neg P \implies Q) \wedge (\neg P \implies \neg Q)) \implies P$ is a tautology.

This rule of logical deduction is called **reductio ad absurdum**.

It is based on the **law of excluded middle**: $P \vee \neg P$ is a tautology.

Method: Assume (let) $\neg P$. Then ... $Q$. Then ... $\neg Q$. Therefore, $P$.

**Example 1.** Prove that $\sqrt{2}$ is irrational.

**Proof.** The statement to prove:

# Proof by contradiction (indirect proof)

Idea: To prove $P$, we assume $\neg P$ and get two mutually exclusive statements, $Q$ and $\neg Q$.

Logical justification: $(\neg P \implies Q) \wedge (\neg P \implies \neg Q)) \implies P$ is a tautology.

This rule of logical deduction is called **reductio ad absurdum**.

It is based on the **law of excluded middle**: $P \vee \neg P$ is a tautology.

Method: Assume (let) $\neg P$. Then ... $Q$. Then ... $\neg Q$. Therefore, $P$.

**Example 1.** Prove that $\sqrt{2}$ is irrational.

**Proof.** The statement to prove: $\boxed{\sqrt{2} \text{ is irrational}}$.

# Proof by contradiction (indirect proof)

Idea: To prove $P$, we assume $\neg P$ and get two mutually exclusive statements, $Q$ and $\neg Q$.

Logical justification: $(\neg P \implies Q) \wedge (\neg P \implies \neg Q)) \implies P$ is a tautology.

This rule of logical deduction is called **reductio ad absurdum**.

It is based on the **law of excluded middle**: $P \vee \neg P$ is a tautology.

Method: Assume (let) $\neg P$. Then ... $Q$. Then ... $\neg Q$. Therefore, $P$.

**Example 1.** Prove that $\sqrt{2}$ is irrational.

**Proof.** The statement to prove: $\underbrace{\boxed{\sqrt{2} \text{ is irrational}}}_{P}$.

# Proof by contradiction (indirect proof)

Idea: To prove $P$, we assume $\neg P$ and get two mutually exclusive statements, $Q$ and $\neg Q$.

Logical justification: $(\neg P \implies Q) \land (\neg P \implies \neg Q)) \implies P$ is a tautology.

This rule of logical deduction is called **reductio ad absurdum**.

It is based on the **law of excluded middle**: $P \lor \neg P$ is a tautology.

Method: Assume (let) $\neg P$. Then ... $Q$. Then ... $\neg Q$. Therefore, $P$.

**Example 1.** Prove that $\sqrt{2}$ is irrational.

**Proof.** The statement to prove: $\underbrace{\boxed{\sqrt{2} \text{ is irrational}}}_{P}$.

Assume, to the contrary, that

## Proof by contradiction (indirect proof)



Idea: To prove $P$, we assume $\neg P$ and get two mutually exclusive statements, $Q$ and $\neg Q$.

Logical justification: $(\neg P \implies Q) \wedge (\neg P \implies \neg Q)) \implies P$ is a tautology.

This rule of logical deduction is called **reductio ad absurdum**.

It is based on the **law of excluded middle**: $P \vee \neg P$ is a tautology.

Method: Assume (let) $\neg P$. Then ... $Q$. Then ... $\neg Q$. Therefore, $P$.

**Example 1.** Prove that $\sqrt{2}$ is irrational.

**Proof.** The statement to prove: $\underbrace{\boxed{\sqrt{2} \text{ is irrational}}}_{P}$.

Assume, to the contrary, that $\boxed{\sqrt{2} \text{ is rational}}$.

# Proof by contradiction (indirect proof)

Idea: To prove $P$, we assume $\neg P$ and get two mutually exclusive statements, $Q$ and $\neg Q$.

Logical justification: $(\neg P \implies Q) \wedge (\neg P \implies \neg Q)) \implies P$ is a tautology.

This rule of logical deduction is called **reductio ad absurdum**.

It is based on the **law of excluded middle**: $P \vee \neg P$ is a tautology.

Method: Assume (let) $\neg P$. Then ... $Q$. Then ... $\neg Q$. Therefore, $P$.

**Example 1.** Prove that $\sqrt{2}$ is irrational.

**Proof.** The statement to prove: $\underbrace{\boxed{\sqrt{2} \text{ is irrational}}}_{P}$.

Assume, to the contrary, that $\underbrace{\boxed{\sqrt{2} \text{ is rational}}}_{\neg P}$.

# Proof by contradiction (indirect proof)

Idea: To prove $P$, we assume $\neg P$ and get two mutually exclusive statements, $Q$ and $\neg Q$.

Logical justification: $(\neg P \implies Q) \wedge (\neg P \implies \neg Q)) \implies P$ is a tautology.

This rule of logical deduction is called **reductio ad absurdum**.

It is based on the **law of excluded middle**: $P \vee \neg P$ is a tautology.

Method: Assume (let) $\neg P$. Then ... $Q$. Then ... $\neg Q$. Therefore, $P$.

**Example 1.** Prove that $\sqrt{2}$ is irrational.

**Proof.** The statement to prove: $\underbrace{\boxed{\sqrt{2} \text{ is irrational}}}_{P}$.

Assume, to the contrary, that $\underbrace{\boxed{\sqrt{2} \text{ is rational}}}_{\neg P}$.

Then $\sqrt{2} = \dfrac{p}{q}$ for some $p, q \in \mathbb{Z},\ q \neq 0$.

# $\sqrt{2}$ is irrational



Since any fraction $\dfrac{p}{q}$ can be reduced to lowest terms,

# $\sqrt{2}$ is irrational



Since any fraction $\frac{p}{q}$ can be reduced to lowest terms,

we may assume, without loss of generality,

# $\sqrt{2}$ is irrational

Since any fraction $\dfrac{p}{q}$ can be reduced to lowest terms,

we may assume, without loss of generality, that $\gcd(p, q) = 1$ .

## $\sqrt{2}$ is irrational



Since any fraction $\dfrac{p}{q}$ can be reduced to lowest terms,

we may assume, without loss of generality, that $\boxed{\gcd(p, q) = 1}$.

# $\sqrt{2}$ is irrational



Since any fraction $\dfrac{p}{q}$ can be reduced to lowest terms,

we may assume, without loss of generality, that $\underbrace{\boxed{\gcd(p,q)=1}}_{Q}$.

## $\sqrt{2}$ is irrational



Since any fraction $\dfrac{p}{q}$ can be reduced to lowest terms,

we may assume, without loss of generality, that $\underbrace{\boxed{\gcd(p,q) = 1}}_{Q}$.

According to our assumption, $\sqrt{2} = \dfrac{p}{q}$ .

# $\sqrt{2}$ is irrational



Since any fraction $\dfrac{p}{q}$ can be reduced to lowest terms,

we may assume, without loss of generality, that $\underbrace{\boxed{\gcd(p,q)=1}}_{Q}$.

According to our assumption, $\sqrt{2}=\dfrac{p}{q}$. By squaring, we get $2=\dfrac{p^2}{q^2}$,

# $\sqrt{2}$ is irrational



Since any fraction $\dfrac{p}{q}$ can be reduced to lowest terms,

we may assume, without loss of generality, that $\underbrace{\boxed{\gcd(p,q)=1}}_{Q}$.

According to our assumption, $\sqrt{2} = \dfrac{p}{q}$. By squaring, we get $2 = \dfrac{p^2}{q^2}$, so $2q^2 = p^2$.

# $\sqrt{2}$ is irrational

Since any fraction $\dfrac{p}{q}$ can be reduced to lowest terms,

we may assume, without loss of generality, that $\underbrace{\boxed{\gcd(p,q)=1}}_{Q}$.

According to our assumption, $\sqrt{2}=\dfrac{p}{q}$. By squaring, we get $2=\dfrac{p^2}{q^2}$, so $2q^2=p^2$.

It means that $p^2$ is even.

# $\sqrt{2}$ is irrational

Since any fraction $\frac{p}{q}$ can be reduced to lowest terms,

we may assume, without loss of generality, that $\underbrace{\boxed{\gcd(p,q)=1}}_{Q}$.

According to our assumption, $\sqrt{2} = \frac{p}{q}$. By squaring, we get $2 = \frac{p^2}{q^2}$, so $2q^2 = p^2$.

It means that $p^2$ is even. Since $p$ has the same parity as $p^2$

# $\sqrt{2}$ is irrational



Since any fraction $\dfrac{p}{q}$ can be reduced to lowest terms,

we may assume, without loss of generality, that $\underbrace{\boxed{\gcd(p,q)=1}}_{Q}$.

According to our assumption, $\sqrt{2} = \dfrac{p}{q}$. By squaring, we get $2 = \dfrac{p^2}{q^2}$, so $2q^2 = p^2$.

It means that $p^2$ is even. Since $p$ has the same parity as $p^2$
(see Theorem about the same parity of an integer and its square),

# $\sqrt{2}$ is irrational

Since any fraction $\frac{p}{q}$ can be reduced to lowest terms,

we may assume, without loss of generality, that $\underbrace{\boxed{\gcd(p,q)=1}}_{Q}$.

According to our assumption, $\sqrt{2}=\frac{p}{q}$. By squaring, we get $2=\frac{p^2}{q^2}$, so $2q^2=p^2$.

It means that $p^2$ is even. Since $p$ has the same parity as $p^2$ (see Theorem about the same parity of an integer and its square), we conclude that $p$ should be even,

# $\sqrt{2}$ is irrational



Since any fraction $\dfrac{p}{q}$ can be reduced to lowest terms,

we may assume, without loss of generality, that $\underbrace{\boxed{\gcd(p,q)=1}}_{Q}$.

According to our assumption, $\sqrt{2} = \dfrac{p}{q}$. By squaring, we get $2 = \dfrac{p^2}{q^2}$, so $2q^2 = p^2$.

It means that $p^2$ is even. Since $p$ has the same parity as $p^2$ (see Theorem about the same parity of an integer and its square), we conclude that $p$ should be even, that is, $p = 2k$ for some integer $k$.

# $\sqrt{2}$ is irrational



Since any fraction $\frac{p}{q}$ can be reduced to lowest terms,

we may assume, without loss of generality, that $\underbrace{\boxed{\gcd(p,q)=1}}_{Q}$.

According to our assumption, $\sqrt{2} = \frac{p}{q}$. By squaring, we get $2 = \frac{p^2}{q^2}$, so $2q^2 = p^2$.

It means that $p^2$ is even. Since $p$ has the same parity as $p^2$
(see Theorem about the same parity of an integer and its square),
we conclude that $p$ should be even, that is, $p = 2k$ for some integer $k$.

In this case, the identity $2q^2 = p^2$

# $\sqrt{2}$ is irrational



Since any fraction $\frac{p}{q}$ can be reduced to lowest terms,

we may assume, without loss of generality, that $\underbrace{\boxed{\gcd(p,q)=1}}_{Q}$.

According to our assumption, $\sqrt{2}=\frac{p}{q}$. By squaring, we get $2=\frac{p^2}{q^2}$, so $2q^2=p^2$.

It means that $p^2$ is even. Since $p$ has the same parity as $p^2$ (see Theorem about the same parity of an integer and its square), we conclude that $p$ should be even, that is, $p=2k$ for some integer $k$.

In this case, the identity $2q^2=p^2$ is equivalent to $2q^2=(2k)^2$,

# $\sqrt{2}$ is irrational

Since any fraction $\dfrac{p}{q}$ can be reduced to lowest terms,

we may assume, without loss of generality, that $\underbrace{\boxed{\gcd(p,q)=1}}_{Q}$.

According to our assumption, $\sqrt{2}=\dfrac{p}{q}$. By squaring, we get $2=\dfrac{p^2}{q^2}$, so $2q^2=p^2$.

It means that $p^2$ is even. Since $p$ has the same parity as $p^2$ (see Theorem about the same parity of an integer and its square), we conclude that $p$ should be even, that is, $p=2k$ for some integer $k$.

In this case, the identity $2q^2=p^2$ is equivalent to $2q^2=(2k)^2$, or $q^2=2k^2$.

# $\sqrt{2}$ is irrational

Since any fraction $\frac{p}{q}$ can be reduced to lowest terms,

we may assume, without loss of generality, that $\underbrace{\boxed{\gcd(p,q)=1}}_{Q}$.

According to our assumption, $\sqrt{2}=\frac{p}{q}$. By squaring, we get $2=\frac{p^2}{q^2}$, so $2q^2=p^2$.

It means that $p^2$ is even. Since $p$ has the same parity as $p^2$
(see Theorem about the same parity of an integer and its square),
we conclude that $p$ should be even, that is, $p=2k$ for some integer $k$.

In this case, the identity $2q^2=p^2$ is equivalent to $2q^2=(2k)^2$, or $q^2=2k^2$.

By this, $q^2$ is even,

# $\sqrt{2}$ is irrational



Since any fraction $\frac{p}{q}$ can be reduced to lowest terms,

we may assume, without loss of generality, that $\underbrace{\boxed{\gcd(p,q)=1}}_{Q}$.

According to our assumption, $\sqrt{2} = \frac{p}{q}$. By squaring, we get $2 = \frac{p^2}{q^2}$, so $2q^2 = p^2$.

It means that $p^2$ is even. Since $p$ has the same parity as $p^2$

(see Theorem about the same parity of an integer and its square),

we conclude that $p$ should be even, that is, $p = 2k$ for some integer $k$.

In this case, the identity $2q^2 = p^2$ is equivalent to $2q^2 = (2k)^2$, or $q^2 = 2k^2$.

By this, $q^2$ is even, and, therefore, $q$ is even too:

# $\sqrt{2}$ is irrational



Since any fraction $\dfrac{p}{q}$ can be reduced to lowest terms,

we may assume, without loss of generality, that $\underbrace{\boxed{\gcd(p,q)=1}}_{Q}$.

According to our assumption, $\sqrt{2}=\dfrac{p}{q}$. By squaring, we get $2=\dfrac{p^2}{q^2}$, so $2q^2=p^2$.

It means that $p^2$ is even. Since $p$ has the same parity as $p^2$

(see Theorem about the same parity of an integer and its square),

we conclude that $p$ should be even, that is, $p=2k$ for some integer $k$.

In this case, the identity $2q^2=p^2$ is equivalent to $2q^2=(2k)^2$, or $q^2=2k^2$.

By this, $q^2$ is even, and, therefore, $q$ is even too: $2\,|\,q$.

# $\sqrt{2}$ is irrational

Since any fraction $\dfrac{p}{q}$ can be reduced to lowest terms,

we may assume, without loss of generality, that $\underbrace{\boxed{\gcd(p,q)=1}}_{Q}$.

According to our assumption, $\sqrt{2}=\dfrac{p}{q}$. By squaring, we get $2=\dfrac{p^2}{q^2}$, so $2q^2=p^2.$

It means that $p^2$ is even. Since $p$ has the same parity as $p^2$
(see Theorem about the same parity of an integer and its square),
we conclude that $p$ should be even, that is, $p=2k$ for some integer $k$.

In this case, the identity $2q^2=p^2$ is equivalent to $2q^2=(2k)^2$, or $q^2=2k^2$.

By this, $q^2$ is even, and, therefore, $q$ is even too: $2\,|\,q$.

But $p$ is also even,

# $\sqrt{2}$ is irrational

Since any fraction $\frac{p}{q}$ can be reduced to lowest terms,

we may assume, without loss of generality, that $\underbrace{\boxed{\gcd(p,q)=1}}_{Q}$.

According to our assumption, $\sqrt{2}=\frac{p}{q}$. By squaring, we get $2=\frac{p^2}{q^2}$, so $2q^2=p^2$.

It means that $p^2$ is even. Since $p$ has the same parity as $p^2$
(see Theorem about the same parity of an integer and its square),
we conclude that $p$ should be even, that is, $p=2k$ for some integer $k$.

In this case, the identity $2q^2=p^2$ is equivalent to $2q^2=(2k)^2$, or $q^2=2k^2$.

By this, $q^2$ is even, and, therefore, $q$ is even too: $2 \mid q$.

But $p$ is also even, that is $2 \mid p$.

# $\sqrt{2}$ is irrational

Since any fraction $\frac{p}{q}$ can be reduced to lowest terms,

we may assume, without loss of generality, that $\underbrace{\boxed{\gcd(p,q)=1}}_{Q}$.

According to our assumption, $\sqrt{2}=\frac{p}{q}$. By squaring, we get $2=\frac{p^2}{q^2}$, so $2q^2=p^2$.

It means that $p^2$ is even. Since $p$ has the same parity as $p^2$
(see Theorem about the same parity of an integer and its square),
we conclude that $p$ should be even, that is, $p=2k$ for some integer $k$.

In this case, the identity $2q^2=p^2$ is equivalent to $2q^2=(2k)^2$, or $q^2=2k^2$.

By this, $q^2$ is even, and, therefore, $q$ is even too: $2 \mid q$.

But $p$ is also even, that is $2 \mid p$. We have got that $2 \mid p$ and $2 \mid q$.

# $\sqrt{2}$ is irrational

Since any fraction $\frac{p}{q}$ can be reduced to lowest terms,

we may assume, without loss of generality, that $\underbrace{\boxed{\gcd(p,q)=1}}_{Q}$.

According to our assumption, $\sqrt{2}=\frac{p}{q}$. By squaring, we get $2=\frac{p^2}{q^2}$, so $2q^2=p^2$.

It means that $p^2$ is even. Since $p$ has the same parity as $p^2$ (see Theorem about the same parity of an integer and its square), we conclude that $p$ should be even, that is, $p=2k$ for some integer $k$.

In this case, the identity $2q^2=p^2$ is equivalent to $2q^2=(2k)^2$, or $q^2=2k^2$.

By this, $q^2$ is even, and, therefore, $q$ is even too: $2\,|\,q$.

But $p$ is also even, that is $2\,|\,p$. We have got that $2\,|\,p$ and $2\,|\,q$.

Therefore, $\gcd(p,q)\neq 1$

# $\sqrt{2}$ is irrational

Since any fraction $\frac{p}{q}$ can be reduced to lowest terms,

we may assume, without loss of generality, that $\boxed{\gcd(p,q)=1}$.
$Q$

According to our assumption, $\sqrt{2}=\frac{p}{q}$. By squaring, we get $2=\frac{p^2}{q^2}$, so $2q^2=p^2$.

It means that $p^2$ is even. Since $p$ has the same parity as $p^2$
(see Theorem about the same parity of an integer and its square),
we conclude that $p$ should be even, that is, $p=2k$ for some integer $k$.

In this case, the identity $2q^2=p^2$ is equivalent to $2q^2=(2k)^2$, or $q^2=2k^2$.

By this, $q^2$ is even, and, therefore, $q$ is even too: $2\,|\,q$.

But $p$ is also even, that is $2\,|\,p$. We have got that $2\,|\,p$ and $2\,|\,q$.

Therefore $\boxed{\gcd(p,q)\neq 1}$,

# $\sqrt{2}$ is irrational

Since any fraction $\dfrac{p}{q}$ can be reduced to lowest terms,

we may assume, without loss of generality, that $\underbrace{\boxed{\gcd(p,q)=1}}_{Q}$.

According to our assumption, $\sqrt{2}=\dfrac{p}{q}$. By squaring, we get $2=\dfrac{p^2}{q^2}$, so $2q^2=p^2$.

It means that $p^2$ is even. Since $p$ has the same parity as $p^2$
(see Theorem about the same parity of an integer and its square),
we conclude that $p$ should be even, that is, $p=2k$ for some integer $k$.

In this case, the identity $2q^2=p^2$ is equivalent to $2q^2=(2k)^2$, or $q^2=2k^2$.

By this, $q^2$ is even, and, therefore, $q$ is even too: $2\,|\,q$.

But $p$ is also even, that is $2\,|\,p$. We have got that $2\,|\,p$ and $2\,|\,q$.

Therefore $\underbrace{\boxed{\gcd(p,q)\neq 1}}_{\neg Q}$,

# $\sqrt{2}$ is irrational



Since any fraction $\dfrac{p}{q}$ can be reduced to lowest terms,

we may assume, without loss of generality, that $\underbrace{\boxed{\gcd(p,q)=1}}_{Q}$.

According to our assumption, $\sqrt{2} = \dfrac{p}{q}$. By squaring, we get $2 = \dfrac{p^2}{q^2}$, so $2q^2 = p^2$.

It means that $p^2$ is even. Since $p$ has the same parity as $p^2$ (see Theorem about the same parity of an integer and its square), we conclude that $p$ should be even, that is, $p = 2k$ for some integer $k$.

In this case, the identity $2q^2 = p^2$ is equivalent to $2q^2 = (2k)^2$, or $q^2 = 2k^2$.

By this, $q^2$ is even, and, therefore, $q$ is even too: $2 \mid q$.

But $p$ is also even, that is $2 \mid p$. We have got that $2 \mid p$ and $2 \mid q$.

Therefore $\underbrace{\boxed{\gcd(p,q) \neq 1}}_{\neg Q}$, which contradicts to the fact that $\gcd(p,q) = 1$.

# $\sqrt{2}$ is irrational

Since any fraction $\frac{p}{q}$ can be reduced to lowest terms,

we may assume, without loss of generality, that $\underbrace{\boxed{\gcd(p,q)=1}}_{Q}$.

According to our assumption, $\sqrt{2}=\frac{p}{q}$. By squaring, we get $2=\frac{p^2}{q^2}$, so $2q^2=p^2$.

It means that $p^2$ is even. Since $p$ has the same parity as $p^2$ (see Theorem about the same parity of an integer and its square), we conclude that $p$ should be even, that is, $p=2k$ for some integer $k$.

In this case, the identity $2q^2=p^2$ is equivalent to $2q^2=(2k)^2$, or $q^2=2k^2$.

By this, $q^2$ is even, and, therefore, $q$ is even too: $2\,|\,q$.

But $p$ is also even, that is $2\,|\,p$. We have got that $2\,|\,p$ and $2\,|\,q$.

Therefore $\underbrace{\boxed{\gcd(p,q)\neq 1}}_{\neg Q}$, which contradicts to the fact that $\gcd(p,q)=1$.

This contradiction shows that the original assumption ( $\sqrt{2}$ is rational)

# $\sqrt{2}$ is irrational

Since any fraction $\frac{p}{q}$ can be reduced to lowest terms,

we may assume, without loss of generality, that $\underbrace{\boxed{\gcd(p,q)=1}}_{Q}$.

According to our assumption, $\sqrt{2}=\frac{p}{q}$. By squaring, we get $2=\frac{p^2}{q^2}$, so $2q^2=p^2$.

It means that $p^2$ is even. Since $p$ has the same parity as $p^2$ (see Theorem about the same parity of an integer and its square), we conclude that $p$ should be even, that is, $p=2k$ for some integer $k$.

In this case, the identity $2q^2=p^2$ is equivalent to $2q^2=(2k)^2$, or $q^2=2k^2$.

By this, $q^2$ is even, and, therefore, $q$ is even too: $2\,|\,q$.

But $p$ is also even, that is $2\,|\,p$. We have got that $2\,|\,p$ and $2\,|\,q$.

Therefore $\underbrace{\boxed{\gcd(p,q)\neq 1}}_{\neg Q}$, which contradicts to the fact that $\gcd(p,q)=1$.

This contradiction shows that the original assumption ($\sqrt{2}$ is rational) was erroneous,

# $\sqrt{2}$ is irrational

Since any fraction $\dfrac{p}{q}$ can be reduced to lowest terms,

we may assume, without loss of generality, that $\underbrace{\boxed{\gcd(p,q)=1}}_{Q}$.

According to our assumption, $\sqrt{2} = \dfrac{p}{q}$. By squaring, we get $2 = \dfrac{p^2}{q^2}$, so $2q^2 = p^2$.

It means that $p^2$ is even. Since $p$ has the same parity as $p^2$
(see Theorem about the same parity of an integer and its square),
we conclude that $p$ should be even, that is, $p = 2k$ for some integer $k$.

In this case, the identity $2q^2 = p^2$ is equivalent to $2q^2 = (2k)^2$, or $q^2 = 2k^2$.

By this, $q^2$ is even, and, therefore, $q$ is even too: $2 \mid q$.

But $p$ is also even, that is $2 \mid p$. We have got that $2 \mid p$ and $2 \mid q$.

Therefore $\underbrace{\boxed{\gcd(p,q) \neq 1}}_{\neg Q}$, which contradicts to the fact that $\gcd(p,q) = 1$.

This contradiction shows that the original assumption ($\sqrt{2}$ is rational) was erroneous,
and $\sqrt{2}$ is actually irrational,

# $\sqrt{2}$ is irrational

Since any fraction $\dfrac{p}{q}$ can be reduced to lowest terms,

we may assume, without loss of generality, that $\underbrace{\boxed{\gcd(p,q)=1}}_{Q}$.

According to our assumption, $\sqrt{2}=\dfrac{p}{q}$. By squaring, we get $2=\dfrac{p^2}{q^2}$, so $2q^2=p^2$.

It means that $p^2$ is even. Since $p$ has the same parity as $p^2$
(see Theorem about the same parity of an integer and its square),
we conclude that $p$ should be even, that is, $p=2k$ for some integer $k$.

In this case, the identity $2q^2=p^2$ is equivalent to $2q^2=(2k)^2$, or $q^2=2k^2$.

By this, $q^2$ is even, and, therefore, $q$ is even too: $2\,|\,q$.

But $p$ is also even, that is $2\,|\,p$. We have got that $2\,|\,p$ and $2\,|\,q$.

Therefore $\underbrace{\boxed{\gcd(p,q)\neq 1}}_{\neg Q}$, which contradicts to the fact that $\gcd(p,q)=1$.

This contradiction shows that the original assumption ($\sqrt{2}$ is rational) was erroneous, and $\sqrt{2}$ is actually irrational, as required.

# Euclid's theorem

# Euclid's theorem

**Theorem (Euclid).** *There are infinitely many prime numbers.*

# Euclid's theorem

**Theorem (Euclid).** *There are infinitely many prime numbers.*

**Proof.**

# Euclid's theorem

**Theorem (Euclid).** *There are infinitely many prime numbers.*

**Proof.** Assume, to the contrary, that there are only finitely many prime numbers:

# Euclid's theorem

**Theorem (Euclid).** *There are infinitely many prime numbers.*

**Proof.** Assume, to the contrary, that there are only finitely many prime numbers:

$$p_1, p_2, \ldots, p_n .$$

# Euclid's theorem



**Theorem (Euclid).** *There are infinitely many prime numbers.*

**Proof.** Assume, to the contrary, that there are only finitely many prime numbers:

$$p_1,\, p_2,\, \ldots,\, p_n\,.$$

Construct a number $N$

# Euclid's theorem

**Theorem (Euclid).** *There are infinitely many prime numbers.*

**Proof.** Assume, to the contrary, that there are only finitely many prime numbers:

$$p_1, p_2, \ldots, p_n.$$

Construct a number $N = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$.

# Euclid's theorem



**Theorem (Euclid).** *There are infinitely many prime numbers.*

**Proof.** Assume, to the contrary, that there are only finitely many prime numbers:

$$p_1, p_2, \ldots, p_n\,.$$

Construct a number $N = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$.

$N$ is not divisible by any of $p_1$,

# Euclid's theorem

**Theorem (Euclid).** *There are infinitely many prime numbers.*

**Proof.** Assume, to the contrary, that there are only finitely many prime numbers:

$$p_1, p_2, \ldots, p_n .$$

Construct a number $N = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$ .

$N$ is not divisible by any of $p_1$ , $p_2$ ,

# Euclid's theorem

**Theorem (Euclid).** *There are infinitely many prime numbers.*

**Proof.** Assume, to the contrary, that there are only finitely many prime numbers:

$$p_1, p_2, \ldots, p_n .$$

Construct a number $N = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$ .

$N$ is not divisible by any of $p_1$ , $p_2$ , $\ldots$ , $p_n$ .

# Euclid's theorem

**Theorem (Euclid).** *There are infinitely many prime numbers.*

**Proof.** Assume, to the contrary, that there are only finitely many prime numbers:

$$p_1, p_2, \ldots, p_n .$$

Construct a number $N = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$ .

$N$ is not divisible by any of $p_1$ , $p_2$ , $\ldots$ , $p_n$ .

Indeed,

# Euclid's theorem



**Theorem (Euclid).** *There are infinitely many prime numbers.*

**Proof.** Assume, to the contrary, that there are only finitely many prime numbers:

$$p_1, p_2, \ldots, p_n .$$

Construct a number $N = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$.

$N$ is not divisible by any of $p_1$, $p_2$, $\ldots$, $p_n$.

Indeed, $N$ has a remainder of $1$ when divided by any of them.

# Euclid's theorem

**Theorem (Euclid).** *There are infinitely many prime numbers.*

**Proof.** Assume, to the contrary, that there are only finitely many prime numbers:

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

Construct a number $N = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$ .

$N$ is not divisible by any of $p_1$ , $p_2$ , $\dots$ , $p_n$ .

Indeed, $N$ has a remainder of $1$ when divided by any of them.

As any natural number greater than $1$ , $N$ is divisible by some prime number.

# Euclid's theorem



**Theorem (Euclid).** *There are infinitely many prime numbers.*

**Proof.** Assume, to the contrary, that there are only finitely many prime numbers:

$$p_1, p_2, \ldots, p_n\,.$$

Construct a number $N = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$.

$N$ is not divisible by any of $p_1$, $p_2$, $\ldots$, $p_n$.

Indeed, $N$ has a remainder of $1$ when divided by any of them.

As any natural number greater than $1$, $N$ is divisible by some prime number.

By this, $N$ should be divisible by one of the primes $p_1, p_2, \ldots, p_n$.

# Euclid's theorem

**Theorem (Euclid).** *There are infinitely many prime numbers.*

**Proof.** Assume, to the contrary, that there are only finitely many prime numbers:

$$p_1, p_2, \ldots, p_n .$$

Construct a number $N = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$ .

$N$ is not divisible by any of $p_1$ , $p_2$ , $\ldots$ , $p_n$ .

Indeed, $N$ has a remainder of $1$ when divided by any of them.

As any natural number greater than $1$ , $N$ is divisible by some prime number.

By this, $N$ should be divisible by one of the primes $p_1, p_2, \ldots, p_n$ .

This contradiction shows that

# Euclid's theorem

**Theorem (Euclid).** *There are infinitely many prime numbers.*

**Proof.** Assume, to the contrary, that there are only finitely many prime numbers:

$$p_1, p_2, \ldots, p_n .$$

Construct a number $N = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$ .

$N$ is not divisible by any of $p_1$ , $p_2$ , $\ldots$ , $p_n$ .

Indeed, $N$ has a remainder of $1$ when divided by any of them.

As any natural number greater than $1$ , $N$ is divisible by some prime number.

By this, $N$ should be divisible by one of the primes $p_1, p_2, \ldots, p_n$ .

This contradiction shows that

the assumption (there are only finitely many prime numbers) was erroneous,

# Euclid's theorem

**Theorem (Euclid).** *There are infinitely many prime numbers.*

**Proof.** Assume, to the contrary, that there are only finitely many prime numbers:

$$p_1, p_2, \ldots, p_n .$$

Construct a number $N = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$ .

$N$ is not divisible by any of $p_1$ , $p_2$ , $\ldots$ , $p_n$ .

Indeed, $N$ has a remainder of $1$ when divided by any of them.

As any natural number greater than $1$ , $N$ is divisible by some prime number.

By this, $N$ should be divisible by one of the primes $p_1, p_2, \ldots, p_n$ .

This contradiction shows that

the assumption (there are only finitely many prime numbers) was erroneous,

and there are infinitely many primes,

# Euclid's theorem

**Theorem (Euclid).** *There are infinitely many prime numbers.*

**Proof.** Assume, to the contrary, that there are only finitely many prime numbers:

$$p_1, p_2, \ldots, p_n .$$

Construct a number $N = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$.

$N$ is not divisible by any of $p_1$, $p_2$, $\ldots$, $p_n$.
Indeed, $N$ has a remainder of $1$ when divided by any of them.
As any natural number greater than $1$, $N$ is divisible by some prime number.

By this, $N$ should be divisible by one of the primes $p_1, p_2, \ldots, p_n$.
This contradiction shows that
the assumption (there are only finitely many prime numbers) was erroneous, and there are infinitely many primes, as required.

# Euclid's theorem

**Theorem (Euclid).** *There are infinitely many prime numbers.*

**Proof.** Assume, to the contrary, that there are only finitely many prime numbers:

$$p_1, p_2, \ldots, p_n.$$

Construct a number $N = p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$.

$N$ is not divisible by any of $p_1$, $p_2$, $\ldots$, $p_n$.

Indeed, $N$ has a remainder of $1$ when divided by any of them.

As any natural number greater than $1$, $N$ is divisible by some prime number.

By this, $N$ should be divisible by one of the primes $p_1, p_2, \ldots, p_n$.

This contradiction shows that

the assumption (there are only finitely many prime numbers) was erroneous, and there are infinitely many primes, as required.

For source and comments see

**Euclid's Elements**, Book IX, Proposition 20.

# How Euclid wrote this

https://mathcs.clarku.edu/~djoyce/java/elements/bookIX/propIX20.html

**Elements**, Book IX, Proposition 20.

## How Euclid wrote this

https://mathcs.clarku.edu/~djoyce/java/elements/bookIX/propIX20.html

**Elements**, Book IX, Proposition 20.

**Prime numbers are more than any assigned multitude of prime numbers.**

# How Euclid wrote this



https://mathcs.clarku.edu/~djoyce/java/elements/bookIX/propIX20.html
**Elements**, Book IX, Proposition 20.

**Prime numbers are more than any assigned multitude of prime numbers.**

Let $A$, $B$, and $C$ be the assigned prime numbers.

# How Euclid wrote this

https://mathcs.clarku.edu/~djoyce/java/elements/bookIX/propIX20.html
**Elements**, Book IX, Proposition 20.

**Prime numbers are more than any assigned multitude of prime numbers.**

Let $A$, $B$, and $C$ be the assigned prime numbers.

I say that there are more prime numbers than $A$, $B$, and $C$.

# How Euclid wrote this



https://mathcs.clarku.edu/~djoyce/java/elements/bookIX/propIX20.html
**Elements**, Book IX, Proposition 20.

**Prime numbers are more than any assigned multitude of prime numbers.**

Let $A$, $B$, and $C$ be the assigned prime numbers.

I say that there are more prime numbers than $A$, $B$, and $C$.

Take the least number $DE$ measured by $A$, $B$, and $C$. Add the unit $DF$ to $DE$.

# How Euclid wrote this

https://mathcs.clarku.edu/~djoyce/java/elements/bookIX/propIX20.html
**Elements**, Book IX, Proposition 20.

**Prime numbers are more than any assigned multitude of prime numbers.**

Let $A$, $B$, and $C$ be the assigned prime numbers.

I say that there are more prime numbers than $A$, $B$, and $C$.

Take the least number $DE$ measured by $A$, $B$, and $C$. Add the unit $DF$ to $DE$. Then $EF$ is either prime or not.

# How Euclid wrote this



https://mathcs.clarku.edu/~djoyce/java/elements/bookIX/propIX20.html

**Elements**, Book IX, Proposition 20.

**Prime numbers are more than any assigned multitude of prime numbers.**

Let $A$, $B$, and $C$ be the assigned prime numbers.

I say that there are more prime numbers than $A$, $B$, and $C$.

Take the least number $DE$ measured by $A$, $B$, and $C$. Add the unit $DF$ to $DE$.
Then $EF$ is either prime or not.
First, let it be prime. Then the prime numbers $A, B, C$, and $EF$ have been found which are more than $A, B$, and $C$.

# How Euclid wrote this



https://mathcs.clarku.edu/~djoyce/java/elements/bookIX/propIX20.html
**Elements**, Book IX, Proposition 20.

**Prime numbers are more than any assigned multitude of prime numbers.**

Let $A$, $B$, and $C$ be the assigned prime numbers.

I say that there are more prime numbers than $A$, $B$, and $C$.

Take the least number $DE$ measured by $A$, $B$, and $C$. Add the unit $DF$ to $DE$.
Then $EF$ is either prime or not.
First, let it be prime. Then the prime numbers $A, B, C$, and $EF$ have been found which are more than $A, B$, and $C$.
Next, let $EF$ not be prime. Therefore it is measured by some prime number. Let it be measured by the prime number $G$.

# How Euclid wrote this

https://mathcs.clarku.edu/~djoyce/java/elements/bookIX/propIX20.html
**Elements**, Book IX, Proposition 20.

**Prime numbers are more than any assigned multitude of prime numbers.**

Let $A$, $B$, and $C$ be the assigned prime numbers.

I say that there are more prime numbers than $A$, $B$, and $C$.

Take the least number $DE$ measured by $A$, $B$, and $C$. Add the unit $DF$ to $DE$.
Then $EF$ is either prime or not.
First, let it be prime. Then the prime numbers $A, B, C$, and $EF$ have been found which are more than $A, B$, and $C$.
Next, let $EF$ not be prime. Therefore it is measured by some prime number. Let it be measured by the prime number $G$.
I say that $G$ is not the same with any of the numbers $A, B$, and $C$.

# How Euclid wrote this



https://mathcs.clarku.edu/~djoyce/java/elements/bookIX/propIX20.html
**Elements**, Book IX, Proposition 20.

**Prime numbers are more than any assigned multitude of prime numbers.**

Let $A$, $B$, and $C$ be the assigned prime numbers.

I say that there are more prime numbers than $A$, $B$, and $C$.

Take the least number $DE$ measured by $A$, $B$, and $C$. Add the unit $DF$ to $DE$.
Then $EF$ is either prime or not.
First, let it be prime. Then the prime numbers $A, B, C$, and $EF$ have been found which are more than $A, B$, and $C$.
Next, let $EF$ not be prime. Therefore it is measured by some prime number. Let it be measured by the prime number $G$.
I say that $G$ is not the same with any of the numbers $A, B$, and $C$.
If possible, let it be so. Now $A$, $B$, and $C$ measure $DE$, therefore $G$ also measures $DE$.

# Proof by exhaustion (proof by cases)

# Proof by exhaustion (proof by cases)

A proof by exhaustion consists of examination of every possible case.

# Proof by exhaustion (proof by cases)



A proof by exhaustion consists of examination of every possible case.

**Inscribed Angle Theorem.** *An angle inscribed in a circle is half of the central angle subtending the same arc.*

## Proof by exhaustion (proof by cases)

A proof by exhaustion consists of examination of every possible case.

**Inscribed Angle Theorem.** *An angle inscribed in a circle is half of the central angle subtending the same arc.*

**Proof.**

## Proof by exhaustion (proof by cases)

A proof by exhaustion consists of examination of every possible case.

**Inscribed Angle Theorem.** *An angle inscribed in a circle is half of the central angle subtending the same arc.*

**Proof.** How an inscribed angle may be positioned with respect to the center of the circle?

# Proof by exhaustion (proof by cases)

A proof by exhaustion consists of examination of every possible case.

**Inscribed Angle Theorem.** *An angle inscribed in a circle is half of the central angle subtending the same arc.*

**Proof.** How an inscribed angle may be positioned with respect to the center of the circle?

Listen to the proof and try to write it down...

# The triangle inequality

# The triangle inequality



**Theorem (triangle inequality).** $|a+b| \leq |a| + |b|$ *for any real numbers* $a, b$.

# The triangle inequality



**Theorem (triangle inequality).** $|a+b| \leq |a| + |b|$ *for any real numbers* $a, b$.

**Proof**

# The triangle inequality

**Theorem (triangle inequality).** $|a+b| \leq |a| + |b|$ *for any real numbers* $a, b$.

**Proof** (by cases).

# The triangle inequality

**Theorem (triangle inequality).** $|a+b| \leq |a| + |b|$ *for any real numbers* $a, b$ *.*

**Proof** (by cases).

- Case 1. $a \geq 0$ and $b \geq 0$ .

# The triangle inequality

**Theorem (triangle inequality).** $|a+b| \leq |a|+|b|$ *for any real numbers* $a, b$ *.*

**Proof** (by cases).

- Case 1. $a \geq 0$ and $b \geq 0$ .Then $|a| = a$ , $|b| = b$ , $|a+b| = a+b$ ,

# The triangle inequality

**Theorem (triangle inequality).** $|a+b| \leq |a| + |b|$ *for any real numbers* $a, b$.

**Proof** (by cases).
• Case 1. $a \geq 0$ and $b \geq 0$ .Then $|a| = a$, $|b| = b$, $|a+b| = a+b$, so
$|a+b| = a+b = |a| + |b|$,

# The triangle inequality



**Theorem (triangle inequality).** $|a+b| \leq |a| + |b|$ *for any real numbers* $a, b$.

**Proof** (by cases).

• Case 1. $a \geq 0$ and $b \geq 0$ .Then $|a| = a$, $|b| = b$, $|a+b| = a+b$, so $|a+b| = a+b = |a| + |b|$, and, by this $|a+b| \leq |a| + |b|$ .

# The triangle inequality

**Theorem (triangle inequality).** $|a+b| \leq |a| + |b|$ *for any real numbers* $a, b$*.*

**Proof** (by cases).

- Case 1. $a \geq 0$ and $b \geq 0$ .Then $|a| = a$, $|b| = b$, $|a+b| = a+b$, so $|a+b| = a+b = |a| + |b|$, and, by this $|a+b| \leq |a| + |b|$ .
- Case 2. $a \geq 0$ and $b < 0$ .

## The triangle inequality



**Theorem (triangle inequality).** $|a+b| \leq |a|+|b|$ *for any real numbers* $a, b$*.*

**Proof** (by cases).

• Case 1. $a \geq 0$ and $b \geq 0$ .Then $|a| = a$, $|b| = b$, $|a+b| = a+b$, so $|a+b| = a+b = |a|+|b|$, and, by this $|a+b| \leq |a|+|b|$ .

• Case 2. $a \geq 0$ and $b < 0$ .Then $|a| = a$, $|b| = -b$,

# The triangle inequality

**Theorem (triangle inequality).** $|a+b| \leq |a| + |b|$ *for any real numbers* $a, b$.

**Proof** (by cases).

- Case 1. $a \geq 0$ and $b \geq 0$ .Then $|a| = a$, $|b| = b$, $|a+b| = a+b$, so $|a+b| = a+b = |a| + |b|$, and, by this $|a+b| \leq |a| + |b|$ .

- Case 2. $a \geq 0$ and $b < 0$ .Then $|a| = a$, $|b| = -b$, $|a+b| =?$

# The triangle inequality

**Theorem (triangle inequality).** $|a+b| \leq |a| + |b|$ *for any real numbers* $a, b$*.*

**Proof** (by cases).

- Case 1. $a \geq 0$ and $b \geq 0$ .Then $|a| = a$, $|b| = b$, $|a+b| = a+b$, so $|a+b| = a+b = |a| + |b|$, and, by this $|a+b| \leq |a| + |b|$ .
- Case 2. $a \geq 0$ and $b < 0$ .Then $|a| = a$, $|b| = -b$, $|a+b| = ?$
    - Case 2a) $a+b \geq 0$.

# The triangle inequality



**Theorem (triangle inequality).** $|a+b| \leq |a|+|b|$ *for any real numbers* $a, b$.

**Proof** (by cases).

- Case 1. $a \geq 0$ and $b \geq 0$ .Then $|a| = a$, $|b| = b$, $|a+b| = a+b$, so $|a+b| = a+b = |a|+|b|$, and, by this $|a+b| \leq |a|+|b|$ .
- Case 2. $a \geq 0$ and $b < 0$ .Then $|a| = a$, $|b| = -b$, $|a+b| =?$
  - Case 2a) $a+b \geq 0$. Then $|a+b| = a+b < a-b = |a|+|b|$,

## The triangle inequality

**Theorem (triangle inequality).** $|a+b| \leq |a|+|b|$ *for any real numbers* $a, b$.

**Proof** (by cases).

- Case 1. $a \geq 0$ and $b \geq 0$ .Then $|a| = a$, $|b| = b$, $|a+b| = a+b$, so $|a+b| = a+b = |a|+|b|$, and, by this $|a+b| \leq |a|+|b|$ .
- Case 2. $a \geq 0$ and $b < 0$ .Then $|a| = a$, $|b| = -b$, $|a+b| =?$
  - Case 2a) $a+b \geq 0$. Then $|a+b| = a+b < a-b = |a|+|b|$, so $|a+b| \leq |a|+|b|$.

## The triangle inequality

**Theorem (triangle inequality).** $|a+b| \leq |a|+|b|$ *for any real numbers* $a, b$.

**Proof** (by cases).

- Case 1. $a \geq 0$ and $b \geq 0$ .Then $|a| = a$, $|b| = b$, $|a+b| = a+b$, so $|a+b| = a+b = |a|+|b|$, and, by this $|a+b| \leq |a|+|b|$ .
- Case 2. $a \geq 0$ and $b < 0$ .Then $|a| = a$, $|b| = -b$, $|a+b| =?$
  - Case 2a) $a+b \geq 0$. Then $|a+b| = a+b < a-b = |a|+|b|$, so $|a+b| \leq |a|+|b|$.
  - Case 2b) $a+b < 0$.

# The triangle inequality

**Theorem (triangle inequality).** $|a+b| \leq |a| + |b|$ *for any real numbers* $a, b$.

**Proof** (by cases).

• Case 1. $a \geq 0$ and $b \geq 0$ .Then $|a| = a$, $|b| = b$, $|a+b| = a+b$, so $|a+b| = a+b = |a| + |b|$, and, by this $|a+b| \leq |a| + |b|$ .

• Case 2. $a \geq 0$ and $b < 0$ .Then $|a| = a$, $|b| = -b$, $|a+b| = ?$

• Case 2a) $a+b \geq 0$. Then $|a+b| = a+b < a-b = |a| + |b|$, so $|a+b| \leq |a| + |b|$.

• Case 2b) $a+b < 0$. Then $|a+b| = -a-b \leq a-b = |a| + |b|$,

# The triangle inequality

**Theorem (triangle inequality).** $|a+b| \le |a| + |b|$ *for any real numbers* $a, b$.

**Proof** (by cases).

- Case 1. $a \ge 0$ and $b \ge 0$ .Then $|a| = a$, $|b| = b$, $|a+b| = a+b$, so $|a+b| = a+b = |a| + |b|$, and, by this $|a+b| \le |a| + |b|$ .
- Case 2. $a \ge 0$ and $b < 0$ .Then $|a| = a$, $|b| = -b$, $|a+b| = ?$
  - Case 2a) $a+b \ge 0$. Then $|a+b| = a+b < a-b = |a| + |b|$, so $|a+b| \le |a| + |b|$.
  - Case 2b) $a+b < 0$. Then $|a+b| = -a-b \le a-b = |a| + |b|$, so $|a+b| \le |a| + |b|$.

# The triangle inequality

**Theorem (triangle inequality).** $|a+b| \leq |a|+|b|$ *for any real numbers* $a, b$.

**Proof** (by cases).

- Case 1. $a \geq 0$ and $b \geq 0$ .Then $|a| = a$ , $|b| = b$, $|a+b| = a+b$, so $|a+b| = a+b = |a|+|b|$, and, by this $|a+b| \leq |a|+|b|$ .

- Case 2. $a \geq 0$ and $b < 0$ .Then $|a| = a$ , $|b| = -b$, $|a+b| =?$

  - Case 2a) $a+b \geq 0$. Then $|a+b| = a+b < a-b = |a|+|b|$, so $|a+b| \leq |a|+|b|$.

  - Case 2b) $a+b < 0$. Then $|a+b| = -a-b \leq a-b = |a|+|b|$, so $|a+b| \leq |a|+|b|$.

- Case 3. $a < 0$ and $b \geq 0$

# The triangle inequality

**Theorem (triangle inequality).** $|a+b| \leq |a|+|b|$ *for any real numbers* $a, b$*.*

**Proof** (by cases).

- Case 1. $a \geq 0$ and $b \geq 0$ .Then $|a| = a$, $|b| = b$, $|a+b| = a+b$, so $|a+b| = a+b = |a|+|b|$, and, by this $|a+b| \leq |a|+|b|$ .
- Case 2. $a \geq 0$ and $b < 0$ .Then $|a| = a$, $|b| = -b$, $|a+b| = ?$
  - Case 2a) $a+b \geq 0$. Then $|a+b| = a+b < a-b = |a|+|b|$, so $|a+b| \leq |a|+|b|$.
  - Case 2b) $a+b < 0$. Then $|a+b| = -a-b \leq a-b = |a|+|b|$, so $|a+b| \leq |a|+|b|$.
- Case 3. $a < 0$ and $b \geq 0$ is similar to Case 2, just swap $a$ and $b$.

# The triangle inequality

**Theorem (triangle inequality).** $|a+b| \leq |a|+|b|$ *for any real numbers* $a, b$*.*

**Proof** (by cases).

- Case 1. $a \geq 0$ and $b \geq 0$ .Then $|a| = a$, $|b| = b$, $|a+b| = a+b$, so $|a+b| = a+b = |a|+|b|$, and, by this $|a+b| \leq |a|+|b|$ .

- Case 2. $a \geq 0$ and $b < 0$ .Then $|a| = a$, $|b| = -b$, $|a+b| =?$

  - Case 2a) $a+b \geq 0$. Then $|a+b| = a+b < a-b = |a|+|b|$, so $|a+b| \leq |a|+|b|$.

  - Case 2b) $a+b < 0$. Then $|a+b| = -a-b \leq a-b = |a|+|b|$, so $|a+b| \leq |a|+|b|$.

- Case 3. $a < 0$ and $b \geq 0$ is similar to Case 2, just swap $a$ and $b$.

- Case 4. $a < 0$ and $b < 0$ .

# The triangle inequality

**Theorem (triangle inequality).** $|a+b| \leq |a|+|b|$ *for any real numbers* $a, b$*.*

**Proof** (by cases).

• Case 1. $a \geq 0$ and $b \geq 0$ .Then $|a| = a$, $|b| = b$, $|a+b| = a+b$, so $|a+b| = a+b = |a|+|b|$, and, by this $|a+b| \leq |a|+|b|$ .

• Case 2. $a \geq 0$ and $b < 0$ .Then $|a| = a$, $|b| = -b$, $|a+b| =?$

• Case 2a) $a+b \geq 0$. Then $|a+b| = a+b < a-b = |a|+|b|$, so $|a+b| \leq |a|+|b|$.

• Case 2b) $a+b < 0$. Then $|a+b| = -a-b \leq a-b = |a|+|b|$, so $|a+b| \leq |a|+|b|$.

• Case 3. $a < 0$ and $b \geq 0$ is similar to Case 2, just swap $a$ and $b$.

• Case 4. $a < 0$ and $b < 0$ .Then $|a| = -a$, $|b| = -b$, $|a+b| = -a-b$,

**Theorem (triangle inequality).** $|a+b| \leq |a|+|b|$ *for any real numbers* $a, b$.

**Proof** (by cases).

• Case 1. $a \geq 0$ and $b \geq 0$ .Then $|a| = a$, $|b| = b$, $|a+b| = a+b$, so $|a+b| = a+b = |a|+|b|$, and, by this $|a+b| \leq |a|+|b|$ .

• Case 2. $a \geq 0$ and $b < 0$ .Then $|a| = a$, $|b| = -b$, $|a+b| =?$

• Case 2a) $a+b \geq 0$. Then $|a+b| = a+b < a-b = |a|+|b|$, so $|a+b| \leq |a|+|b|$.

• Case 2b) $a+b < 0$. Then $|a+b| = -a-b \leq a-b = |a|+|b|$, so $|a+b| \leq |a|+|b|$.

• Case 3. $a < 0$ and $b \geq 0$ is similar to Case 2, just swap $a$ and $b$.

• Case 4. $a < 0$ and $b < 0$ .Then $|a| = -a$, $|b| = -b$, $|a+b| = -a-b$, so $|a+b| = -a-b = |a|+|b|$,

# The triangle inequality

**Theorem (triangle inequality).** $|a+b| \leq |a|+|b|$ *for any real numbers* $a, b$.

**Proof** (by cases).

- Case 1. $a \geq 0$ and $b \geq 0$ .Then $|a|=a$, $|b|=b$, $|a+b|=a+b$, so $|a+b|=a+b=|a|+|b|$, and, by this $|a+b| \leq |a|+|b|$ .

- Case 2. $a \geq 0$ and $b<0$ .Then $|a|=a$, $|b|=-b$, $|a+b|=?$

  - Case 2a) $a+b \geq 0$. Then $|a+b|=a+b<a-b=|a|+|b|$, so $|a+b| \leq |a|+|b|$.

  - Case 2b) $a+b<0$. Then $|a+b|=-a-b \leq a-b=|a|+|b|$, so $|a+b| \leq |a|+|b|$.

- Case 3. $a<0$ and $b \geq 0$ is similar to Case 2, just swap $a$ and $b$.

- Case 4. $a<0$ and $b<0$ .Then $|a|=-a$, $|b|=-b$, $|a+b|=-a-b$, so $|a+b|=-a-b=|a|+|b|$, and, by this $|a+b| \leq |a|+|b|$ .

## The triangle inequality

**Theorem (triangle inequality).** $|a+b| \leq |a|+|b|$ *for any real numbers* $a, b$.

**Proof** (by cases).

• Case 1. $a \geq 0$ and $b \geq 0$ .Then $|a|=a$, $|b|=b$, $|a+b|=a+b$, so $|a+b|=a+b=|a|+|b|$, and, by this $|a+b| \leq |a|+|b|$ .

• Case 2. $a \geq 0$ and $b < 0$ .Then $|a|=a$, $|b|=-b$, $|a+b| = ?$

• Case 2a) $a+b \geq 0$. Then $|a+b|=a+b<a-b=|a|+|b|$, so $|a+b| \leq |a|+|b|$.

• Case 2b) $a+b<0$. Then $|a+b|=-a-b \leq a-b=|a|+|b|$, so $|a+b| \leq |a|+|b|$.

• Case 3. $a<0$ and $b \geq 0$ is similar to Case 2, just swap $a$ and $b$.

• Case 4. $a<0$ and $b<0$ .Then $|a|=-a$, $|b|=-b$, $|a+b|=-a-b$, so $|a+b|=-a-b=|a|+|b|$, and, by this $|a+b| \leq |a|+|b|$ .

Therefore, $|a+b| \leq |a|+|b|$ for all real numbers $a$ and $b$,

# The triangle inequality

**Theorem (triangle inequality).** $|a+b| \leq |a| + |b|$ *for any real numbers* $a, b$.

**Proof** (by cases).

• Case 1. $a \geq 0$ and $b \geq 0$ .Then $|a| = a$, $|b| = b$, $|a+b| = a+b$, so $|a+b| = a+b = |a| + |b|$, and, by this $|a+b| \leq |a| + |b|$ .

• Case 2. $a \geq 0$ and $b < 0$ .Then $|a| = a$, $|b| = -b$, $|a+b| =?$

• Case 2a) $a+b \geq 0$. Then $|a+b| = a+b < a-b = |a| + |b|$, so $|a+b| \leq |a| + |b|$.

• Case 2b) $a+b < 0$. Then $|a+b| = -a-b \leq a-b = |a| + |b|$, so $|a+b| \leq |a| + |b|$.

• Case 3. $a < 0$ and $b \geq 0$ is similar to Case 2, just swap $a$ and $b$.

• Case 4. $a < 0$ and $b < 0$ .Then $|a| = -a$, $|b| = -b$, $|a+b| = -a-b$, so $|a+b| = -a-b = |a| + |b|$, and, by this $|a+b| \leq |a| + |b|$ .

Therefore, $|a+b| \leq |a| + |b|$ for all real numbers $a$ and $b$, as required.

# The triangle inequality

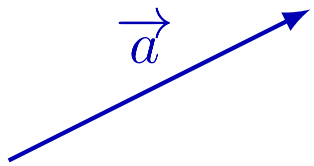
# The triangle inequality



Why the inequality $|a + b| \leq |a| + |b|$ is called the **triangle inequality**?

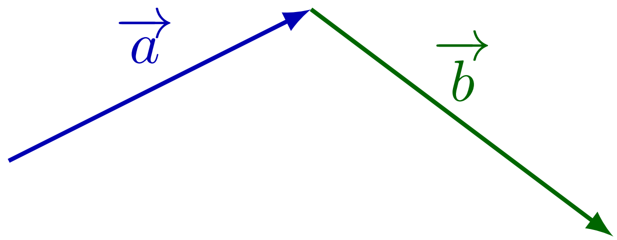
# The triangle inequality

Why the inequality $|a + b| \leq |a| + |b|$ is called the **triangle inequality**?



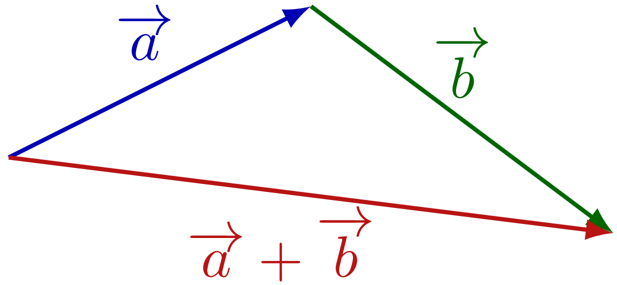
# The triangle inequality

Why the inequality $|a+b| \leq |a| + |b|$ is called the **triangle inequality**?



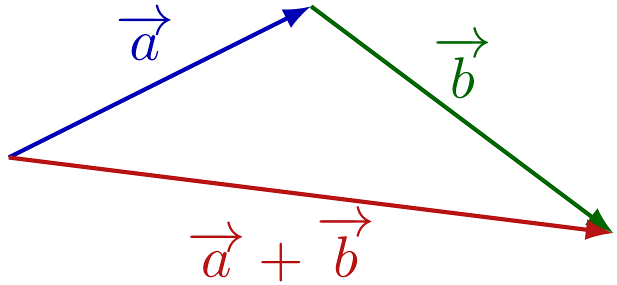
# The triangle inequality

Why the inequality $|a+b| \leq |a| + |b|$ is called the **triangle inequality**?



# The triangle inequality

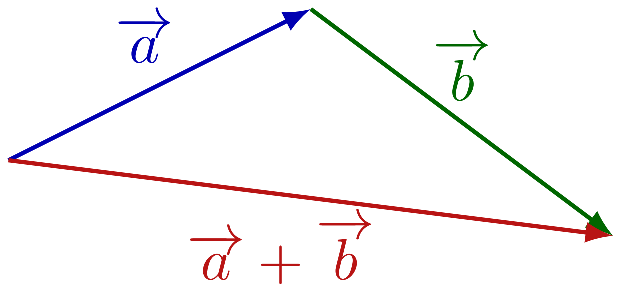
Why the inequality $|a+b| \leq |a| + |b|$ is called the **triangle inequality**?




$$|\overrightarrow{a} + \overrightarrow{b}| < |\overrightarrow{a}| + |\overrightarrow{b}|$$

# The triangle inequality

Why the inequality $|a+b| \leq |a| + |b|$ is called the **triangle inequality**?

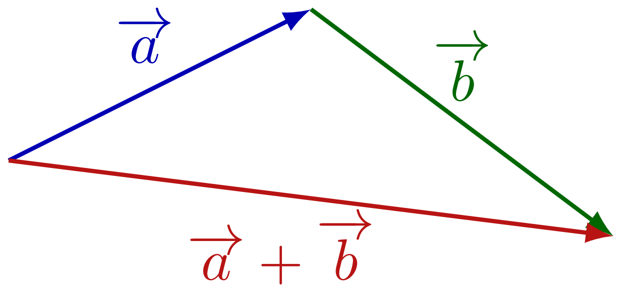



$|\overrightarrow{a} + \overrightarrow{b}| < |\overrightarrow{a}| + |\overrightarrow{b}|$

**Corollary 1.** $|a-b| \leq |a| + |b|$ for all $a, b \in \mathbb{R}$.

# The triangle inequality

Why the inequality $|a+b| \leq |a| + |b|$ is called the **triangle inequality**?




$$|\overrightarrow{a} + \overrightarrow{b}| < |\overrightarrow{a}| + |\overrightarrow{b}|$$

**Corollary 1.** $|a-b| \leq |a| + |b|$ for all $a, b \in \mathbb{R}$.

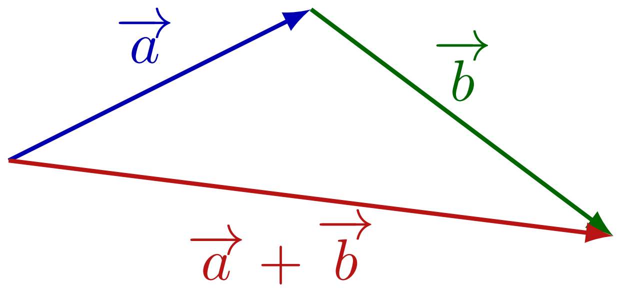
**Proof.** Apply the triangle inequality to $a$ and $-b$:

.

.

# The triangle inequality

Why the inequality $|a+b| \leq |a|+|b|$ is called the **triangle inequality**?



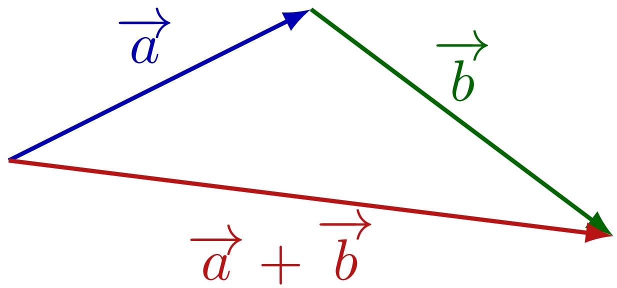

$$|\overrightarrow{a}+\overrightarrow{b}| < |\overrightarrow{a}| + |\overrightarrow{b}|$$

**Corollary 1.** $|a-b| \leq |a|+|b|$ for all $a, b \in \mathbb{R}$.

**Proof.** Apply the triangle inequality to $a$ and $-b$:
$|a+(-b)| \leq |a| + |-b|$.

# The triangle inequality

Why the inequality $|a+b| \leq |a| + |b|$ is called the **triangle inequality**?




$|\overrightarrow{a} + \overrightarrow{b}| < |\overrightarrow{a}| + |\overrightarrow{b}|$

**Corollary 1.** $|a-b| \leq |a| + |b|$ for all $a, b \in \mathbb{R}$.

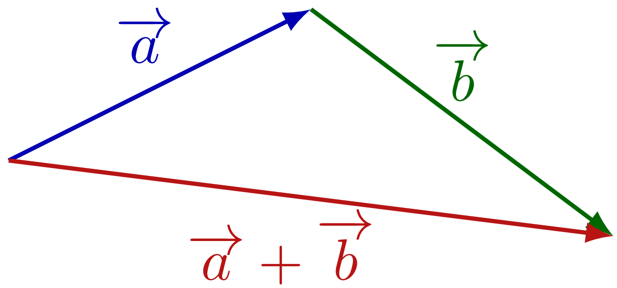
**Proof.** Apply the triangle inequality to $a$ and $-b$:
$|a+(-b)| \leq |a| + |-b|$.
Since $a+(-b) = a-b$ and $|-b| = |b|$,

.

.

# The triangle inequality

Why the inequality $|a+b| \le |a| + |b|$ is called the **triangle inequality**?



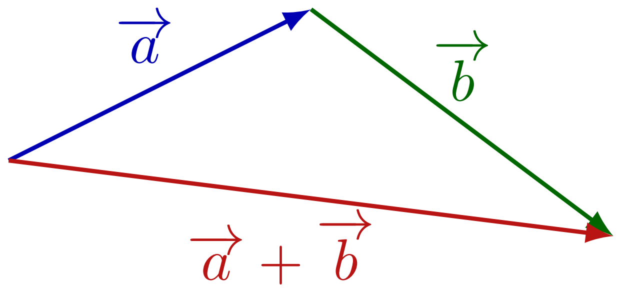

$|\overrightarrow{a} + \overrightarrow{b}| < |\overrightarrow{a}| + |\overrightarrow{b}|$

**Corollary 1.** $|a-b| \le |a| + |b|$ for all $a, b \in \mathbb{R}$.

**Proof.** Apply the triangle inequality to $a$ and $-b$:
$|a + (-b)| \le |a| + |-b|$.
Since $a + (-b) = a - b$ and $|-b| = |b|$,
we have got $|a-b| \le |a| + |b|$, as required.

# The triangle inequality

Why the inequality $|a+b| \leq |a| + |b|$ is called the **triangle inequality**?




$$|\overrightarrow{a} + \overrightarrow{b}| < |\overrightarrow{a}| + |\overrightarrow{b}|$$

**Corollary 1.** $|a-b| \leq |a| + |b|$ for all $a, b \in \mathbb{R}$.

**Proof.** Apply the triangle inequality to $a$ and $-b$:
$|a+(-b)| \leq |a| + |-b|$.
Since $a+(-b) = a-b$ and $|-b| = |b|$,
we have got $|a-b| \leq |a| + |b|$, as required.

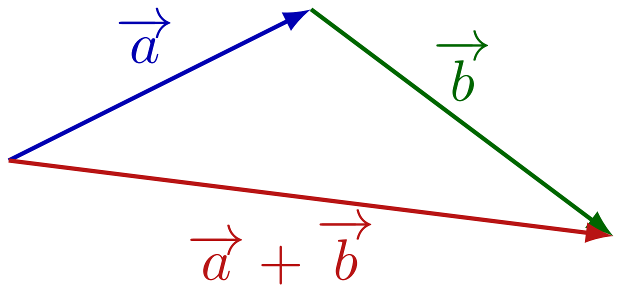
**Corollary 2.** $||a| - |b|| \leq |a-b|$ for all $a, b \in \mathbb{R}$.

.

.

# The triangle inequality

Why the inequality $|a+b| \le |a| + |b|$ is called the **triangle inequality**?




$$|\overrightarrow{a} + \overrightarrow{b}| < |\overrightarrow{a}| + |\overrightarrow{b}|$$

**Corollary 1.** $|a-b| \le |a| + |b|$ for all $a, b \in \mathbb{R}$.

**Proof.** Apply the triangle inequality to $a$ and $-b$:
$|a + (-b)| \le |a| + |-b|$.
Since $a + (-b) = a - b$ and $|-b| = |b|$,
we have got $|a-b| \le |a| + |b|$, as required.

**Corollary 2.** $||a| - |b|| \le |a-b|$ for all $a, b \in \mathbb{R}$.

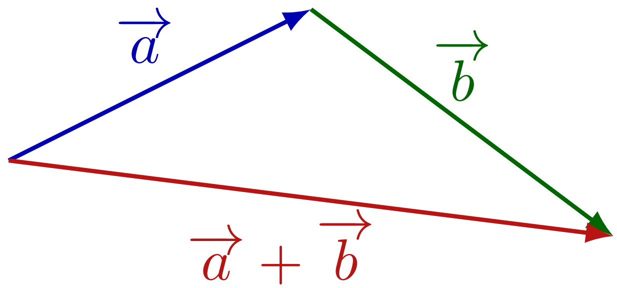
**Proof.** $|a| = |(a-b) + b|$

.

.

# The triangle inequality

Why the inequality $|a+b| \leq |a| + |b|$ is called the **triangle inequality**?




$$|\overrightarrow{a} + \overrightarrow{b}| < |\overrightarrow{a}| + |\overrightarrow{b}|$$

**Corollary 1.** $|a-b| \leq |a| + |b|$ for all $a, b \in \mathbb{R}$.

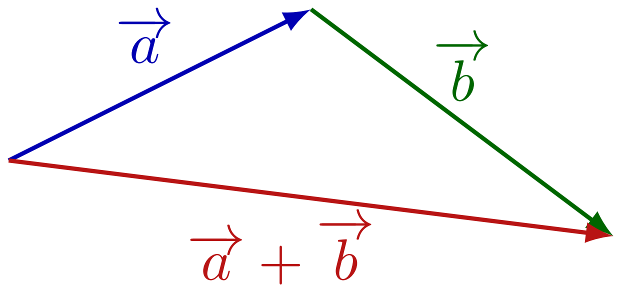
**Proof.** Apply the triangle inequality to $a$ and $-b$:
$|a + (-b)| \leq |a| + |-b|$.
Since $a + (-b) = a - b$ and $|-b| = |b|$,
we have got $|a-b| \leq |a| + |b|$, as required.

**Corollary 2.** $||a| - |b|| \leq |a-b|$ for all $a, b \in \mathbb{R}$.

**Proof.** $|a| = |(a-b) + b| \leq |a-b| + |b|$

# The triangle inequality

Why the inequality $|a+b| \le |a| + |b|$ is called the **triangle inequality**?




$$|\overrightarrow{a} + \overrightarrow{b}| < |\overrightarrow{a}| + |\overrightarrow{b}|$$

**Corollary 1.** $|a-b| \le |a| + |b|$ for all $a, b \in \mathbb{R}$.

**Proof.** Apply the triangle inequality to $a$ and $-b$:
$|a+(-b)| \le |a| + |-b|$.
Since $a+(-b) = a-b$ and $|-b| = |b|$,
we have got $|a-b| \le |a| + |b|$, as required.

**Corollary 2.** $||a| - |b|| \le |a-b|$ for all $a, b \in \mathbb{R}$.

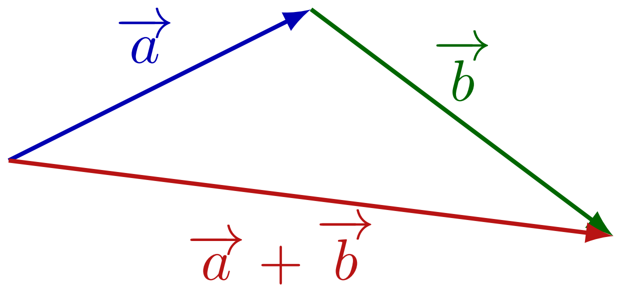
**Proof.** $|a| = |(a-b)+b| \le |a-b| + |b| \implies |a| - |b| \le |a-b|$.

.

.

# The triangle inequality

Why the inequality $|a+b| \le |a| + |b|$ is called the **triangle inequality**?




$$|\overrightarrow{a} + \overrightarrow{b}| < |\overrightarrow{a}| + |\overrightarrow{b}|$$

**Corollary 1.** $|a-b| \le |a| + |b|$ for all $a, b \in \mathbb{R}$.

**Proof.** Apply the triangle inequality to $a$ and $-b$:
$|a+(-b)| \le |a| + |-b|$.
Since $a+(-b) = a-b$ and $|-b| = |b|$,
we have got $|a-b| \le |a| + |b|$, as required.

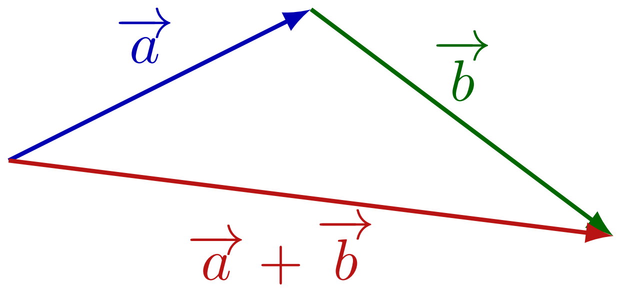
**Corollary 2.** $||a| - |b|| \le |a-b|$ for all $a, b \in \mathbb{R}$.

**Proof.** $|a| = |(a-b)+b| \le |a-b| + |b| \implies |a| - |b| \le |a-b|$.
$|b| = |(b-a)+a| \le |b-a| + |a| \implies |a| - |b| \ge -|a-b|$.

.

# The triangle inequality

Why the inequality $|a+b| \leq |a| + |b|$ is called the **triangle inequality**?




$|\overrightarrow{a} + \overrightarrow{b}| < |\overrightarrow{a}| + |\overrightarrow{b}|$

**Corollary 1.** $|a-b| \leq |a| + |b|$ for all $a, b \in \mathbb{R}$.

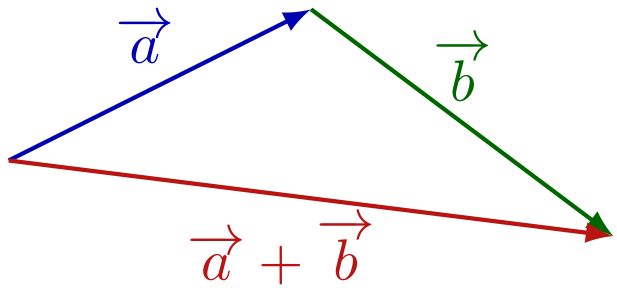
**Proof.** Apply the triangle inequality to $a$ and $-b$:
$|a+(-b)| \leq |a| + |-b|$.
Since $a+(-b) = a-b$ and $|-b| = |b|$,
we have got $|a-b| \leq |a| + |b|$, as required.

**Corollary 2.** $||a| - |b|| \leq |a-b|$ for all $a, b \in \mathbb{R}$.

**Proof.** $|a| = |(a-b)+b| \leq |a-b| + |b| \implies |a| - |b| \leq |a-b|$.
$|b| = |(b-a)+a| \leq |b-a| + |a| \implies |a| - |b| \geq -|a-b|$.
Therefore, $-|a-b| \leq |a| - |b| \leq |a-b|$.

# The triangle inequality

Why the inequality $|a+b| \le |a| + |b|$ is called the **triangle inequality**?




$|\overrightarrow{a} + \overrightarrow{b}| < |\overrightarrow{a}| + |\overrightarrow{b}|$

**Corollary 1.** $|a-b| \le |a| + |b|$ for all $a, b \in \mathbb{R}$.

**Proof.** Apply the triangle inequality to $a$ and $-b$:
$|a + (-b)| \le |a| + |-b|$.
Since $a + (-b) = a - b$ and $|-b| = |b|$,
we have got $|a-b| \le |a| + |b|$, as required.

**Corollary 2.** $||a| - |b|| \le |a-b|$ for all $a, b \in \mathbb{R}$.

**Proof.** $|a| = |(a-b) + b| \le |a-b| + |b| \implies |a| - |b| \le |a-b|$.
$|b| = |(b-a) + a| \le |b-a| + |a| \implies |a| - |b| \ge -|a-b|$.
Therefore, $-|a-b| \le |a| - |b| \le |a-b|$. Hence $||a| - |b|| \le |a-b|$, as required.

# The triangle inequality, another proof



Let us give another proof of the triangle inequality.

# The triangle inequality, another proof



Let us give another proof of the triangle inequality.

For any real numbers $a$ and $b$, we have

# The triangle inequality, another proof



Let us give another proof of the triangle inequality.

For any real numbers $a$ and $b$, we have

$(a+b)^2 = a^2 + b^2 + 2ab$

# The triangle inequality, another proof



Let us give another proof of the triangle inequality.

For any real numbers $a$ and $b$, we have

$$(a+b)^2 = a^2 + b^2 + 2ab \underbrace{\leq}_{ab \leq |ab|} a^2 + b^2 + 2|ab|$$

# The triangle inequality, another proof



Let us give another proof of the triangle inequality.

For any real numbers $a$ and $b$, we have

$$(a+b)^2 = a^2 + b^2 + 2ab \underbrace{\leq}_{ab \leq |ab|} a^2 + b^2 + 2|ab| = |a|^2 + |b|^2 + 2|a||b|$$

# The triangle inequality, another proof



Let us give another proof of the triangle inequality.

For any real numbers $a$ and $b$, we have

$$(a+b)^2 = a^2+b^2+2ab \underbrace{\leq}_{ab\leq|ab|} a^2+b^2+2|ab| = |a|^2+|b|^2+2|a||b| = (|a|+|b|)^2 .$$

# The triangle inequality, another proof



Let us give another proof of the triangle inequality.

For any real numbers $a$ and $b$, we have

$$(a+b)^2 = a^2+b^2+2ab \underbrace{\leq}_{ab\leq|ab|} a^2+b^2+2|ab| = |a|^2+|b|^2+2|a||b| = (|a|+|b|)^2 .$$

Therefore, $(a+b)^2 \leq (|a|+|b|)^2$ .

# The triangle inequality, another proof



Let us give another proof of the triangle inequality.

For any real numbers $a$ and $b$, we have

$$(a+b)^2 = a^2+b^2+2ab \underbrace{\leq}_{ab\leq|ab|} a^2+b^2+2|ab| = |a|^2+|b|^2+2|a||b| = (|a|+|b|)^2\,.$$

Therefore, $(a+b)^2 \leq (|a|+|b|)^2$. From this we get

# The triangle inequality, another proof

Let us give another proof of the triangle inequality.

For any real numbers $a$ and $b$, we have

$$(a+b)^2 = a^2+b^2+2ab \underbrace{\leq}_{ab\leq|ab|} a^2+b^2+2|ab| = |a|^2+|b|^2+2|a||b| = (|a|+|b|)^2 .$$

Therefore, $(a+b)^2 \leq (|a|+|b|)^2$. From this we get

$$\sqrt{(a+b)^2} \leq \sqrt{(|a|+|b|)^2} ,$$

# The triangle inequality, another proof



Let us give another proof of the triangle inequality.

For any real numbers $a$ and $b$, we have

$$(a+b)^2 = a^2+b^2+2ab \underbrace{\leq}_{ab\leq|ab|} a^2+b^2+2|ab| = |a|^2+|b|^2+2|a||b| = (|a|+|b|)^2 .$$

Therefore, $(a+b)^2 \leq (|a|+|b|)^2$. From this we get

$\sqrt{(a+b)^2} \leq \sqrt{(|a|+|b|)^2}$, which implies

$|a+b| \leq ||a|+|b||$.

## The triangle inequality, another proof



Let us give another proof of the triangle inequality.

For any real numbers $a$ and $b$, we have

$$(a+b)^2 = a^2+b^2+2ab \underbrace{\leq}_{ab\leq|ab|} a^2+b^2+2|ab| = |a|^2+|b|^2+2|a||b| = (|a|+|b|)^2 .$$

Therefore, $(a+b)^2 \leq (|a|+|b|)^2$. From this we get

$\sqrt{(a+b)^2} \leq \sqrt{(|a|+|b|)^2}$, which implies
$|a+b| \leq ||a|+|b||$.

Since $||a|+|b||| = |a|+|b|$,

# The triangle inequality, another proof



Let us give another proof of the triangle inequality.

For any real numbers $a$ and $b$, we have

$$(a+b)^2 = a^2+b^2+2ab \underbrace{\leq}_{ab\leq|ab|} a^2+b^2+2|ab| = |a|^2+|b|^2+2|a||b| = (|a|+|b|)^2 .$$

Therefore, $(a+b)^2 \leq (|a|+|b|)^2$. From this we get

$\sqrt{(a+b)^2} \leq \sqrt{(|a|+|b|)^2}$, which implies

$|a+b| \leq ||a|+|b||$.

Since $||a|+|b||| = |a|+|b|$, we get $|a+b| \leq |a|+|b|$.

# How to prove an equivalence

# How to prove an equivalence

To prove a statement of type $P \iff Q$,

# How to prove an equivalence



To prove a statement of type $P \iff Q$, we may use one of two alternatives:

# How to prove an equivalence

To prove a statement of type $P \iff Q$, we may use one of two alternatives:

Alternative 1: $P$

# How to prove an equivalence

To prove a statement of type $P \iff Q$, we may use one of two alternatives:

Alternative 1: $P \iff R$

# How to prove an equivalence



To prove a statement of type $P \iff Q$, we may use one of two alternatives:

Alternative 1: $P \iff R \iff S$

# How to prove an equivalence



To prove a statement of type $P \iff Q$, we may use one of two alternatives:

Alternative 1: $P \iff R \iff S \iff \cdots \iff Q$

## How to prove an equivalence



To prove a statement of type $P \iff Q$, we may use one of two alternatives:

Alternative 1: $P \iff R \iff S \iff \cdots \iff Q$

Alternative 2: $P \implies Q$

# How to prove an equivalence

To prove a statement of type $P \iff Q$, we may use one of two alternatives:

Alternative 1: $P \iff R \iff S \iff \cdots \iff Q$

Alternative 2: $P \implies Q$ and $Q \implies P$.

# How to prove an equivalence



To prove a statement of type $P \iff Q$, we may use one of two alternatives:

Alternative 1: $P \iff R \iff S \iff \cdots \iff Q$

Alternative 2: $P \implies Q$ and $Q \implies P$.

**Example 1.**

# How to prove an equivalence



To prove a statement of type $P \iff Q$, we may use one of two alternatives:

Alternative 1: $P \iff R \iff S \iff \cdots \iff Q$

Alternative 2: $P \implies Q$ and $Q \implies P$.

**Example 1.** Let $a, b, c$ be the lengths of the sides of a triangle

# How to prove an equivalence



To prove a statement of type $P \iff Q$, we may use one of two alternatives:

Alternative 1: $P \iff R \iff S \iff \cdots \iff Q$

Alternative 2: $P \implies Q$ and $Q \implies P$.

**Example 1.** Let $a, b, c$ be the lengths of the sides of a triangle and $a \leq b \leq c$.

# How to prove an equivalence

To prove a statement of type $P \iff Q$, we may use one of two alternatives:

Alternative 1: $P \iff R \iff S \iff \cdots \iff Q$

Alternative 2: $P \implies Q$ and $Q \implies P$.

**Example 1.** Let $a, b, c$ be the lengths of the sides of a triangle and $a \leq b \leq c$. Using the law of cosines, prove that the triangle is right if and only if $a^2 + b^2 = c^2$.

# How to prove an equivalence



To prove a statement of type $P \iff Q$, we may use one of two alternatives:

Alternative 1: $P \iff R \iff S \iff \cdots \iff Q$

Alternative 2: $P \implies Q$ and $Q \implies P$.

**Example 1.** Let $a, b, c$ be the lengths of the sides of a triangle and $a \leq b \leq c$. Using the law of cosines, prove that the triangle is right if and only if $a^2 + b^2 = c^2$.

**Proof.** What is the law of cosines?

# How to prove an equivalence

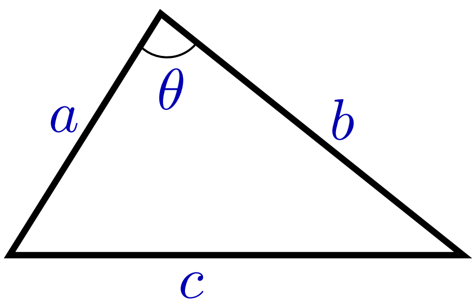
To prove a statement of type $P \iff Q$, we may use one of two alternatives:

Alternative 1: $P \iff R \iff S \iff \cdots \iff Q$

Alternative 2: $P \implies Q$ and $Q \implies P$.

**Example 1.** Let $a, b, c$ be the lengths of the sides of a triangle and $a \leq b \leq c$. Using the law of cosines, prove that the triangle is right if and only if $a^2 + b^2 = c^2$.

**Proof.** What is the law of cosines?



# How to prove an equivalence

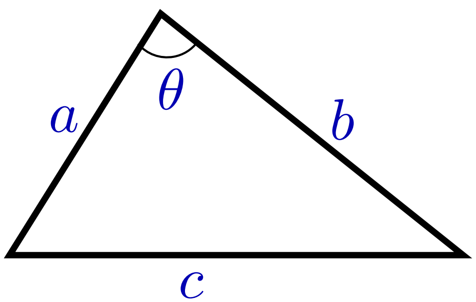
To prove a statement of type $P \iff Q$, we may use one of two alternatives:

Alternative 1: $P \iff R \iff S \iff \cdots \iff Q$

Alternative 2: $P \implies Q$ and $Q \implies P$.

**Example 1.** Let $a, b, c$ be the lengths of the sides of a triangle and $a \leq b \leq c$. Using the law of cosines, prove that the triangle is right if and only if $a^2 + b^2 = c^2$.

**Proof.** What is the law of cosines?




$$c^2 = a^2 + b^2 - 2ab\cos\theta$$

# How to prove an equivalence

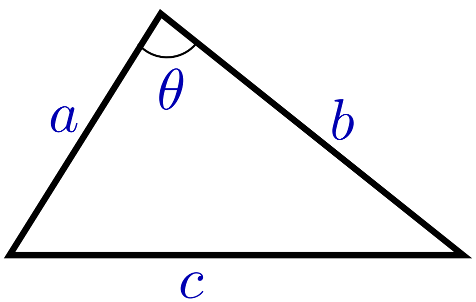
To prove a statement of type $P \iff Q$, we may use one of two alternatives:

Alternative 1: $P \iff R \iff S \iff \cdots \iff Q$

Alternative 2: $P \implies Q$ and $Q \implies P$.

**Example 1.** Let $a, b, c$ be the lengths of the sides of a triangle and $a \leq b \leq c$. Using the law of cosines, prove that the triangle is right if and only if $a^2 + b^2 = c^2$.

**Proof.** What is the law of cosines?




$$c^2 = a^2 + b^2 - 2ab\cos\theta$$

A triangle with the sides $a, b, c$ is right

## How to prove an equivalence

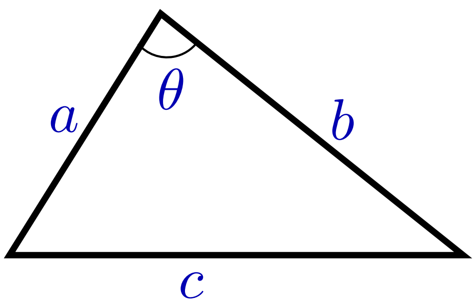
To prove a statement of type $P \iff Q$, we may use one of two alternatives:

Alternative 1: $P \iff R \iff S \iff \cdots \iff Q$

Alternative 2: $P \implies Q$ and $Q \implies P$.

**Example 1.** Let $a, b, c$ be the lengths of the sides of a triangle and $a \leq b \leq c$. Using the law of cosines, prove that the triangle is right if and only if $a^2 + b^2 = c^2$.

**Proof.** What is the law of cosines?




$$c^2 = a^2 + b^2 - 2ab\cos\theta$$

A triangle with the sides $a, b, c$ is right $\underset{?}{\iff}$ $\theta = 90^\circ$

# How to prove an equivalence

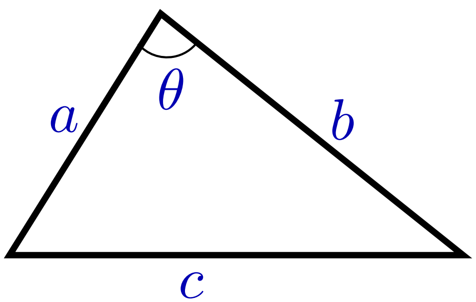
To prove a statement of type $P \iff Q$, we may use one of two alternatives:

Alternative 1: $P \iff R \iff S \iff \cdots \iff Q$

Alternative 2: $P \implies Q$ and $Q \implies P$.

**Example 1.** Let $a, b, c$ be the lengths of the sides of a triangle and $a \le b \le c$. Using the law of cosines, prove that the triangle is right if and only if $a^2 + b^2 = c^2$.

**Proof.** What is the law of cosines?




$$c^2 = a^2 + b^2 - 2ab\cos\theta$$

A triangle with the sides $a, b, c$ is right $\underset{?}{\iff}$ $\theta = 90^\circ$ $\underset{?}{\iff}$ $\cos\theta = 0$

# How to prove an equivalence

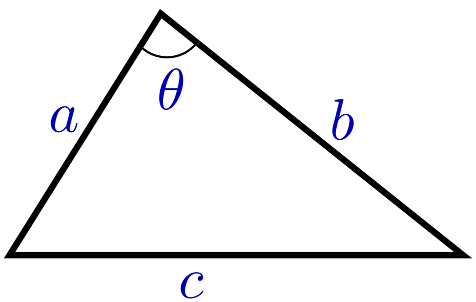
To prove a statement of type $P \iff Q$, we may use one of two alternatives:

Alternative 1: $P \iff R \iff S \iff \cdots \iff Q$

Alternative 2: $P \implies Q$ and $Q \implies P$.

**Example 1.** Let $a, b, c$ be the lengths of the sides of a triangle and $a \leq b \leq c$. Using the law of cosines, prove that the triangle is right if and only if $a^2 + b^2 = c^2$.

**Proof.** What is the law of cosines?




$$c^2 = a^2 + b^2 - 2ab\cos\theta$$

A triangle with the sides $a, b, c$ is right $\underset{?}{\iff}$ $\theta = 90^\circ$ $\underset{?}{\iff}$ $\cos\theta = 0$

$$\underset{?}{\iff} c^2 = a^2 + b^2 .$$

# An integer and its cube have the same parity

# An integer and its cube have the same parity



**Example 2.** Let $n$ be an integer.

# An integer and its cube have the same parity

**Example 2.** Let $n$ be an integer. Prove that $n$ is even iff $n^3$ is even.

# An integer and its cube have the same parity



**Example 2.** Let $n$ be an integer. Prove that $n$ is even iff $n^3$ is even.

**Proof.** Let us prove first that

$$n \text{ is even} \implies n^3 \text{ is even.}$$

# An integer and its cube have the same parity

**Example 2.** Let $n$ be an integer. Prove that $n$ is even iff $n^3$ is even.

**Proof.** Let us prove first that

$$n \text{ is even} \implies n^3 \text{ is even.}$$

Let $n$ be even,

# An integer and its cube have the same parity



**Example 2.** Let $n$ be an integer. Prove that $n$ is even iff $n^3$ is even.

**Proof.** Let us prove first that

$$n \text{ is even } \implies n^3 \text{ is even.}$$

Let $n$ be even, so $n = 2k$ for some $k \in \mathbb{Z}$.

# An integer and its cube have the same parity

**Example 2.** Let $n$ be an integer. Prove that $n$ is even iff $n^3$ is even.

**Proof.** Let us prove first that

$$n \text{ is even } \implies n^3 \text{ is even.}$$

Let $n$ be even, so $n = 2k$ for some $k \in \mathbb{Z}$. Then $n^3 = 8k^3$,

# An integer and its cube have the same parity



**Example 2.** Let $n$ be an integer. Prove that $n$ is even iff $n^3$ is even.

**Proof.** Let us prove first that

$$n \text{ is even} \implies n^3 \text{ is even.}$$

Let $n$ be even, so $n = 2k$ for some $k \in \mathbb{Z}$. Then $n^3 = 8k^3$, which is even.

## An integer and its cube have the same parity



**Example 2.** Let $n$ be an integer. Prove that $n$ is even iff $n^3$ is even.

**Proof.** Let us prove first that

$$n \text{ is even} \implies n^3 \text{ is even.}$$

Let $n$ be even, so $n = 2k$ for some $k \in \mathbb{Z}$. Then $n^3 = 8k^3$, which is even.

Let us prove now that

$$n^3 \text{ is even} \implies n \text{ is even.}$$

# An integer and its cube have the same parity



**Example 2.** Let $n$ be an integer. Prove that $n$ is even iff $n^3$ is even.

**Proof.** Let us prove first that

$$n \text{ is even } \implies n^3 \text{ is even.}$$

Let $n$ be even, so $n = 2k$ for some $k \in \mathbb{Z}$. Then $n^3 = 8k^3$, which is even.

Let us prove now that

$$n^3 \text{ is even } \implies n \text{ is even.}$$

Assume that $n$ is odd.

# An integer and its cube have the same parity



**Example 2.** Let $n$ be an integer. Prove that $n$ is even iff $n^3$ is even.

**Proof.** Let us prove first that

$$n \text{ is even} \implies n^3 \text{ is even.}$$

Let $n$ be even, so $n = 2k$ for some $k \in \mathbb{Z}$. Then $n^3 = 8k^3$, which is even.

Let us prove now that

$$n^3 \text{ is even} \implies n \text{ is even.}$$

Assume that $n$ is odd. Then $n = 2k + 1$ for some $k \in \mathbb{Z}$.

# An integer and its cube have the same parity

**Example 2.** Let $n$ be an integer. Prove that $n$ is even iff $n^3$ is even.

**Proof.** Let us prove first that

$$n \text{ is even} \implies n^3 \text{ is even.}$$

Let $n$ be even, so $n = 2k$ for some $k \in \mathbb{Z}$. Then $n^3 = 8k^3$, which is even.

Let us prove now that

$$n^3 \text{ is even} \implies n \text{ is even.}$$

Assume that $n$ is odd. Then $n = 2k + 1$ for some $k \in \mathbb{Z}$. In this case,
$n^3 = (2k + 1)^3 =$

# An integer and its cube have the same parity

**Example 2.** Let $n$ be an integer. Prove that $n$ is even iff $n^3$ is even.

**Proof.** Let us prove first that

$$n \text{ is even } \implies n^3 \text{ is even.}$$

Let $n$ be even, so $n = 2k$ for some $k \in \mathbb{Z}$. Then $n^3 = 8k^3$, which is even.

Let us prove now that

$$n^3 \text{ is even } \implies n \text{ is even.}$$

Assume that $n$ is odd. Then $n = 2k + 1$ for some $k \in \mathbb{Z}$. In this case,
$n^3 = (2k+1)^3 = 8k^3 + 12k^2 + 6k + 1$

# An integer and its cube have the same parity



**Example 2.** Let $n$ be an integer. Prove that $n$ is even iff $n^3$ is even.

**Proof.** Let us prove first that

$$n \text{ is even} \implies n^3 \text{ is even.}$$

Let $n$ be even, so $n = 2k$ for some $k \in \mathbb{Z}$. Then $n^3 = 8k^3$, which is even.

Let us prove now that

$$n^3 \text{ is even} \implies n \text{ is even.}$$

Assume that $n$ is odd. Then $n = 2k + 1$ for some $k \in \mathbb{Z}$. In this case,
$n^3 = (2k+1)^3 = 8k^3 + 12k^2 + 6k + 1 = 2(4k^3 + 6k^2 + 3k) + 1$,

# An integer and its cube have the same parity



**Example 2.** Let $n$ be an integer. Prove that $n$ is even iff $n^3$ is even.

**Proof.** Let us prove first that

$$n \text{ is even} \implies n^3 \text{ is even.}$$

Let $n$ be even, so $n = 2k$ for some $k \in \mathbb{Z}$. Then $n^3 = 8k^3$, which is even.

Let us prove now that

$$n^3 \text{ is even} \implies n \text{ is even.}$$

Assume that $n$ is odd. Then $n = 2k + 1$ for some $k \in \mathbb{Z}$. In this case, $n^3 = (2k+1)^3 = 8k^3 + 12k^2 + 6k + 1 = 2(4k^3 + 6k^2 + 3k) + 1$, which is odd.

# An integer and its cube have the same parity



**Example 2.** Let $n$ be an integer. Prove that $n$ is even iff $n^3$ is even.

**Proof.** Let us prove first that

$$n \text{ is even} \implies n^3 \text{ is even.}$$

Let $n$ be even, so $n = 2k$ for some $k \in \mathbb{Z}$. Then $n^3 = 8k^3$, which is even.

Let us prove now that

$$n^3 \text{ is even} \implies n \text{ is even.}$$

Assume that $n$ is odd. Then $n = 2k + 1$ for some $k \in \mathbb{Z}$. In this case, $n^3 = (2k+1)^3 = 8k^3 + 12k^2 + 6k + 1 = 2(4k^3 + 6k^2 + 3k) + 1$, which is odd. We have got that $n$ is odd $\implies$ $n^3$ is odd.

# An integer and its cube have the same parity

**Example 2.** Let $n$ be an integer. Prove that $n$ is even iff $n^3$ is even.

**Proof.** Let us prove first that

$$n \text{ is even} \implies n^3 \text{ is even.}$$

Let $n$ be even, so $n = 2k$ for some $k \in \mathbb{Z}$. Then $n^3 = 8k^3$, which is even.

Let us prove now that

$$n^3 \text{ is even} \implies n \text{ is even.}$$

Assume that $n$ is odd. Then $n = 2k + 1$ for some $k \in \mathbb{Z}$. In this case, $n^3 = (2k+1)^3 = 8k^3 + 12k^2 + 6k + 1 = 2(4k^3 + 6k^2 + 3k) + 1$, which is odd. We have got that $n$ is odd $\implies n^3$ is odd. Therefore, by contraposition,

# An integer and its cube have the same parity

**Example 2.** Let $n$ be an integer. Prove that $n$ is even iff $n^3$ is even.

**Proof.** Let us prove first that

$$n \text{ is even } \implies n^3 \text{ is even.}$$

Let $n$ be even, so $n = 2k$ for some $k \in \mathbb{Z}$. Then $n^3 = 8k^3$, which is even.

Let us prove now that

$$n^3 \text{ is even } \implies n \text{ is even.}$$

Assume that $n$ is odd. Then $n = 2k + 1$ for some $k \in \mathbb{Z}$. In this case, $n^3 = (2k+1)^3 = 8k^3 + 12k^2 + 6k + 1 = 2(4k^3 + 6k^2 + 3k) + 1$, which is odd. We have got that $n$ is odd $\implies n^3$ is odd. Therefore, by contraposition,

$$n^3 \text{ is even } \implies n \text{ is even.}$$

# An integer and its cube have the same parity

**Example 2.** Let $n$ be an integer. Prove that $n$ is even iff $n^3$ is even.

**Proof.** Let us prove first that

$$n \text{ is even} \implies n^3 \text{ is even.}$$

Let $n$ be even, so $n = 2k$ for some $k \in \mathbb{Z}$. Then $n^3 = 8k^3$, which is even.

Let us prove now that

$$n^3 \text{ is even} \implies n \text{ is even.}$$

Assume that $n$ is odd. Then $n = 2k + 1$ for some $k \in \mathbb{Z}$. In this case, $n^3 = (2k+1)^3 = 8k^3 + 12k^2 + 6k + 1 = 2(4k^3 + 6k^2 + 3k) + 1$, which is odd. We have got that $n$ is odd $\implies n^3$ is odd. Therefore, by contraposition,

$$n^3 \text{ is even} \implies n \text{ is even.}$$

qed

# How to prove uniqueness

# How to prove uniqueness



In order to prove that an object is unique,

# How to prove uniqueness



In order to prove that an object is unique,

one assumes that there are two such objects

# How to prove uniqueness



In order to prove that an object is unique,

one assumes that there are two such objects and come to a conclusion that they have to be equal.

# How to prove uniqueness

In order to prove that an object is unique,

one assumes that there are two such objects and come to a conclusion that they have to be equal.

**Example.**

# How to prove uniqueness

In order to prove that an object is unique,

one assumes that there are two such objects and come to a conclusion that they have to be equal.

**Example.** Prove that in any ring, the additive identity is unique.

# How to prove uniqueness



In order to prove that an object is unique,

one assumes that there are two such objects and come to a conclusion that they have to be equal.

**Example.** Prove that in any ring, the additive identity is unique.

**Proof.**

# How to prove uniqueness

In order to prove that an object is unique,

one assumes that there are two such objects and come to a conclusion that they have to be equal.

**Example.** Prove that in any ring, the additive identity is unique.

**Proof.** Assume that there are two additive identities,

# How to prove uniqueness



In order to prove that an object is unique,

one assumes that there are two such objects and come to a conclusion that they have to be equal.

**Example.** Prove that in any ring, the additive identity is unique.

**Proof.** Assume that there are two additive identities, $0$ and $0'$.

# How to prove uniqueness



In order to prove that an object is unique,

one assumes that there are two such objects and come to a conclusion that they have to be equal.

**Example.** Prove that in any ring, the additive identity is unique.

**Proof.** Assume that there are two additive identities, $0$ and $0'$. Then

# How to prove uniqueness



In order to prove that an object is unique,

one assumes that there are two such objects and come to a conclusion that they have to be equal.

**Example.** Prove that in any ring, the additive identity is unique.

**Proof.** Assume that there are two additive identities, $0$ and $0'$. Then

$0' = 0' + 0$

# How to prove uniqueness



In order to prove that an object is unique,

one assumes that there are two such objects and come to a conclusion that they have to be equal.

**Example.** Prove that in any ring, the additive identity is unique.

**Proof.** Assume that there are two additive identities, $0$ and $0'$. Then

$0' = 0' + 0$ since $a = a + 0$ for any element $a$ in the ring

# How to prove uniqueness

In order to prove that an object is unique,

one assumes that there are two such objects and come to a conclusion that they have to be equal.

**Example.** Prove that in any ring, the additive identity is unique.

**Proof.** Assume that there are two additive identities, $0$ and $0'$. Then

$0' = 0' + 0$ since $a = a + 0$ for any element $a$ in the ring

$= 0 + 0'$

# How to prove uniqueness



In order to prove that an object is unique,

one assumes that there are two such objects

and come to a conclusion that they have to be equal.

**Example.** Prove that in any ring, the additive identity is unique.

**Proof.** Assume that there are two additive identities, $0$ and $0'$. Then

$0' = 0' + 0$ since $a = a + 0$ for any element $a$ in the ring

$= 0 + 0'$ by commutativity of addition in the ring

# How to prove uniqueness

In order to prove that an object is unique,

one assumes that there are two such objects and come to a conclusion that they have to be equal.

**Example.** Prove that in any ring, the additive identity is unique.

**Proof.** Assume that there are two additive identities, $0$ and $0'$. Then

$0' = 0' + 0$ since $a = a + 0$ for any element $a$ in the ring

$= 0 + 0'$ by commutativity of addition in the ring

$= 0$

# How to prove uniqueness

In order to prove that an object is unique,

one assumes that there are two such objects and come to a conclusion that they have to be equal.

**Example.** Prove that in any ring, the additive identity is unique.

**Proof.** Assume that there are two additive identities, $0$ and $0'$. Then

$0' = 0' + 0$ since $a = a + 0$ for any element $a$ in the ring

$= 0 + 0'$ by commutativity of addition in the ring

$= 0$ since $0'$ is an additive identity:

# How to prove uniqueness



In order to prove that an object is unique,
one assumes that there are two such objects
and come to a conclusion that they have to be equal.

**Example.** Prove that in any ring, the additive identity is unique.

**Proof.** Assume that there are two additive identities, $0$ and $0'$. Then

$0' = 0' + 0$ since $a = a + 0$ for any element $a$ in the ring

$= 0 + 0'$ by commutativity of addition in the ring

$= 0$ since $0'$ is an additive identity: $a + 0' = a$ for any $a$ in the ring.

# How to prove uniqueness

In order to prove that an object is unique,
one assumes that there are two such objects
and come to a conclusion that they have to be equal.

**Example.** Prove that in any ring, the additive identity is unique.

**Proof.** Assume that there are two additive identities, $0$ and $0'$. Then

$0' = 0' + 0$ since $a = a + 0$ for any element $a$ in the ring

$= 0 + 0'$ by commutativity of addition in the ring

$= 0$ since $0'$ is an additive identity: $a + 0' = a$ for any $a$ in the ring.

Therefore, $0' = 0$.

# How to prove uniqueness

In order to prove that an object is unique,

one assumes that there are two such objects and come to a conclusion that they have to be equal.

**Example.** Prove that in any ring, the additive identity is unique.

**Proof.** Assume that there are two additive identities, $0$ and $0'$. Then

$0' = 0' + 0$ since $a = a + 0$ for any element $a$ in the ring

$= 0 + 0'$ by commutativity of addition in the ring

$= 0$ since $0'$ is an additive identity: $a + 0' = a$ for any $a$ in the ring.

Therefore, $0' = 0$.

qed

# Strategies for constructing proofs

# Strategies for constructing proofs

- Understand what is given and what is to be proven.

# Strategies for constructing proofs

- Understand what is given and what is to be proven.
  If you prove an implication,

# Strategies for constructing proofs

- Understand what is given and what is to be proven.
  If you prove an implication, identify the assumption (what is given)

# Strategies for constructing proofs



- Understand what is given and what is to be proven.
  If you prove an implication, identify the assumption (what is given)
  and conclusion (what should be proven).

# Strategies for constructing proofs

- Understand what is given and what is to be proven.
  If you prove an implication, identify the assumption (what is given)
  and conclusion (what should be proven).
- Recall all relevant definitions and theorems in their **precise** form.

## Strategies for constructing proofs

- Understand what is given and what is to be proven.
  If you prove an implication, identify the assumption (what is given)
  and conclusion (what should be proven).
- Recall all relevant definitions and theorems in their **precise** form.
- Do math.

# Strategies for constructing proofs

- Understand what is given and what is to be proven.
  If you prove an implication, identify the assumption (what is given)
  and conclusion (what should be proven).
- Recall all relevant definitions and theorems in their **precise** form.
- Do math. Logic can't replace missing mathematics.

# Strategies for constructing proofs

- Understand what is given and what is to be proven.
  If you prove an implication, identify the assumption (what is given)
  and conclusion (what should be proven).
- Recall all relevant definitions and theorems in their **precise** form.
- Do math. Logic can't replace missing mathematics.
- Put math in a correct logical form.

## Strategies for constructing proofs

- Understand what is given and what is to be proven.
  If you prove an implication, identify the assumption (what is given)
  and conclusion (what should be proven).
- Recall all relevant definitions and theorems in their **precise** form.
- Do math. Logic can't replace missing mathematics.
- Put math in a correct logical form.
- Avoid **typical logical mistakes**:

## Strategies for constructing proofs



- Understand what is given and what is to be proven.
  If you prove an implication, identify the assumption (what is given)
  and conclusion (what should be proven).
- Recall all relevant definitions and theorems in their **precise** form.
- Do math. Logic can't replace missing mathematics.
- Put math in a correct logical form.
- Avoid **typical logical mistakes**:
  1. **Affirming the consequent**

# Strategies for constructing proofs

- Understand what is given and what is to be proven.
  If you prove an implication, identify the assumption (what is given)
  and conclusion (what should be proven).
- Recall all relevant definitions and theorems in their **precise** form.
- Do math. Logic can't replace missing mathematics.
- Put math in a correct logical form.
- Avoid **typical logical mistakes**:
  1. **Affirming the consequent**
     Prove $P \implies Q$.

# Strategies for constructing proofs



- Understand what is given and what is to be proven.
  If you prove an implication, identify the assumption (what is given)
  and conclusion (what should be proven).
- Recall all relevant definitions and theorems in their **precise** form.
- Do math. Logic can't replace missing mathematics.
- Put math in a correct logical form.
- Avoid **typical logical mistakes**:
  **1. Affirming the consequent**
  Prove $P \implies Q$.
  "Proof." Let $Q \dots$

# Strategies for constructing proofs



- Understand what is given and what is to be proven.
  If you prove an implication, identify the assumption (what is given)
  and conclusion (what should be proven).
- Recall all relevant definitions and theorems in their **precise** form.
- Do math. Logic can't replace missing mathematics.
- Put math in a correct logical form.
- Avoid **typical logical mistakes**:
  1. **Affirming the consequent**
     Prove $P \implies Q$.
     "Proof." Let $Q \ldots$
  2. **Denying the antecedent**

# Strategies for constructing proofs

- Understand what is given and what is to be proven.
  If you prove an implication, identify the assumption (what is given)
  and conclusion (what should be proven).
- Recall all relevant definitions and theorems in their **precise** form.
- Do math. Logic can't replace missing mathematics.
- Put math in a correct logical form.
- Avoid **typical logical mistakes**:
  1. **Affirming the consequent**
     Prove $P \implies Q$.
     "Proof." Let $Q \ldots$
  2. **Denying the antecedent**
     Prove $P \implies Q$.

## Strategies for constructing proofs

- Understand what is given and what is to be proven.
  If you prove an implication, identify the assumption (what is given)
  and conclusion (what should be proven).
- Recall all relevant definitions and theorems in their **precise** form.
- Do math. Logic can't replace missing mathematics.
- Put math in a correct logical form.
- Avoid **typical logical mistakes**:
  1. **Affirming the consequent**
     Prove $P \implies Q$.
     "Proof." Let $Q \ldots$
  2. **Denying the antecedent**
     Prove $P \implies Q$.
     "Proof." Let $\neg P \ldots$

## Strategies for constructing proofs

- Understand what is given and what is to be proven.
  If you prove an implication, identify the assumption (what is given)
  and conclusion (what should be proven).
- Recall all relevant definitions and theorems in their **precise** form.
- Do math. Logic can't replace missing mathematics.
- Put math in a correct logical form.
- Avoid **typical logical mistakes**:
  1. **Affirming the consequent**
     Prove $P \implies Q$.
     "Proof." Let $Q \ldots$
  2. **Denying the antecedent**
     Prove $P \implies Q$.
     "Proof." Let $\neg P \ldots$
  3. **Guilt by assumption** (proof by example)

## Strategies for constructing proofs



- Understand what is given and what is to be proven.
  If you prove an implication, identify the assumption (what is given)
  and conclusion (what should be proven).
- Recall all relevant definitions and theorems in their **precise** form.
- Do math. Logic can't replace missing mathematics.
- Put math in a correct logical form.
- Avoid **typical logical mistakes**:
  1. **Affirming the consequent**
     Prove $P \implies Q$.
     "Proof." Let $Q \ldots$
  2. **Denying the antecedent**
     Prove $P \implies Q$.
     "Proof." Let $\neg P \ldots$
  3. **Guilt by assumption** (proof by example)
     $\exists x\, P(x) \implies \forall x\, P(x)$