Discrete Mathematics, Section 002, Spring 2016

Lecture 2: Theorems, Proofs

Zsolt Pajor-Gyulai
zsolt@cims.nyu.edu

Courant Institute of Mathematical Sciences

September 12, 2016

Outline

1 Theorems

2 Proof

What is a theorem?

A theorem is a declarative statement about mathematics for which there is a proof.

In other word it is a sentence that expresses an idea about how something is, that we can assign a value of true or false.

What is a theorem?

A theorem is a declarative statement about mathematics for which there is a proof.

In other word it is a sentence that expresses an idea about how something is, that we can assign a value of true or false.

If a supply of a commodity decreases then its price increases.

What is a theorem?

A theorem is a declarative statement about mathematics for which there is a proof.

In other word it is a sentence that expresses an idea about how something is, that we can assign a value of true or false.

The free acceleration on the surface of the earth is $9.8 m/s^2$.

What is a theorem?

A theorem is a declarative statement about mathematics for which there is a proof.

In other word it is a sentence that expresses an idea about how something is, that we can assign a value of true or false.

In mathematics there are four type of statements.

- **Theorems:** Statements that are known to be true.

What is a theorem?

A theorem is a declarative statement about mathematics for which there is a proof.

In other word it is a sentence that expresses an idea about how something is, that we can assign a value of true or false.

In mathematics there are four type of statements.

- **Theorems:** Statements that are known to be true.

Theorem

If a and b are the length of the legs of a right triangle and c is the length of the hypothenuse, then $a^2 + b^2 = c^2$.

What is a theorem?

A theorem is a declarative statement about mathematics for which there is a proof.

In other word it is a sentence that expresses an idea about how something is, that we can assign a value of true or false.

In mathematics there are four type of statements.

- **Theorems:** Statements that are known to be true.
- **Conjecture:** Statements that we suspect to be true but cannot prove it yet.

What is a theorem?

A theorem is a declarative statement about mathematics for which there is a proof.

In other word it is a sentence that expresses an idea about how something is, that we can assign a value of true or false.

In mathematics there are four type of statements.

- **Theorems:** Statements that are known to be true.
- **Conjecture:** Statements that we suspect to be true but cannot prove it yet.

Twin prime conjecture

There are infinitely many primes p such that $p+2$ is also a prime. (E.g. 47)

What is a theorem?

A theorem is a declarative statement about mathematics for which there is a proof.

In other word it is a sentence that expresses an idea about how something is, that we can assign a value of true or false.

In mathematics there are four type of statements.

- **Theorems:** Statements that are known to be true.
- **Conjecture:** Statements that we suspect to be true but cannot prove it yet.
- **Mistake:** A statement that is false.

What is a theorem?

A theorem is a declarative statement about mathematics for which there is a proof.

In other word it is a sentence that expresses an idea about how something is, that we can assign a value of true or false.

In mathematics there are four type of statements.

- **Theorems:** Statements that are known to be true.
- **Conjecture:** Statements that we suspect to be true but cannot prove it yet.
- **Mistake:** A statement that is false.

Every even number is divisible by three

What is a theorem?

A theorem is a declarative statement about mathematics for which there is a proof.

In other word it is a sentence that expresses an idea about how something is, that we can assign a value of true or false.

In mathematics there are four type of statements.

- **Theorems:** Statements that are known to be true.
- **Conjecture:** Statements that we suspect to be true but cannot prove it yet.
- **Mistake:** A statement that is false.
- **Nonsensical:** A statement that does not make sense.

What is a theorem?

A theorem is a declarative statement about mathematics for which there is a proof.

In other word it is a sentence that expresses an idea about how something is, that we can assign a value of true or false.

In mathematics there are four type of statements.

- **Theorems:** Statements that are known to be true.
- **Conjecture:** Statements that we suspect to be true but cannot prove it yet.
- **Mistake:** A statement that is false.
- **Nonsensical:** A statement that does not make sense.

The root of a triangle is a circle.

The notion of truth

Different disciples have different notion of truth. In most disciples a statement is true if it has some appropriate level of predictive value.

The notion of truth

Different disciples have different notion of truth. In most disciples a statement is true if it has some appropriate level of predictive value.

- **Physics:** A statement is true if it has predictive value.

The free acceleration near the surface of the earth is $9.8 m/s^2$.

- The value 9.8 is an approximation.
- 'Near' is vague.
- The actual value has slight variations near the surface.

The notion of truth

Different disciples have different notion of truth. In most disciples a statement is true if it has some appropriate level of predictive value.

- **Physics:** A statement is true if it has predictive value.

The free acceleration near the surface of the earth is $9.8m/s^2$.

  - The value 9.8 is an approximation.
  - 'Near' is vague.
  - The actual value has slight variations near the surface.

- **Meteorology:**

The weather in Baltimore in July is hot and humid.

  - Definitely not every day every July.

The notion of truth

Different disciples have different notion of truth. In most disciples a statement is true if it has some appropriate level of predictive value or descriptive power.

- **Mathematics:**
  - Much stricter than any other disciples.
  - The only truth is absolute, unconditional and without exception.

Theorem

If a and b are the length of the legs of a right triangle and c is the length of the hypothenuse, then $a^2 + b^2 = c^2$.

The notion of truth

Different disciples have different notion of truth. In most disciples a statement is true if it has some appropriate level of predictive value or descriptive power.

- **Mathematics:**
  - Much stricter than any other disciples.
  - The only truth is absolute, unconditional and without exception.

Theorem

If a and b are the length of the legs of a right triangle and c is the length of the hypothenuse, then $a^2 + b^2 = c^2$*.*

- It is true because we can prove it, not because we measure triangles with a ruler.

The notion of truth

Different disciples have different notion of truth. In most disciples a statement is true if it has some appropriate level of predictive value or descriptive power.

- **Mathematics:**
  - Much stricter than any other disciples.
  - The only truth is absolute, unconditional and without exception.

Theorem

If a and b are the length of the legs of a right triangle and c is the length of the hypothenuse, then $a^2 + b^2 = c^2$.

- It is true because we can prove it, not because we measure triangles with a ruler.

Absolute statements can only be made about abstract objects and therefore mathematics works with these. Then usually our results tell us something about the real world as well.

If A then B. ($A \Rightarrow B$).

If x and y are even integers, then so is $x + y$.

This is not the same as everyday English usage:

If you mow the lawn, then I will pay you 20.

What happens if you don't mow the lawn?

If A then B. ($A \Rightarrow B$).

If x and y are even integers, then so is $x + y$.

This is not the same as everyday English usage:

If you mow the lawn, then I will pay you 20.

What happens if you don't mow the lawn?

- Everyday English: You don't get anything.

If A then B. ($A \Rightarrow B$).

If x and y are even integers, then so is $x + y$.

This is not the same as everyday English usage:

If you mow the lawn, then I will pay you 20.

What happens if you don't mow the lawn?

- Everyday English: You don't get anything.
- Mathematics: No information.

A	B	
True	True	Possible
True	False	Impossible
False	True	Possible
False	False	Possible

If A then B. ($A \Rightarrow B$)

Alternative terminology:

- A implies B.

If A then B. ($A \Rightarrow B$)

Alternative terminology:

- A implies B.
- Whenever A we have B.

If A then B. ($A \Rightarrow B$)

Alternative terminology:

- A implies B.
- Whenever A we have B.
- A is sufficient for B.

If A then B. ($A \Rightarrow B$)

Alternative terminology:

- A implies B.
- Whenever A we have B.
- A is sufficient for B.
- B is necessary for A.

If A then B. ($A \Rightarrow B$)

Alternative terminology:

- A implies B.
- Whenever A we have B.
- A is sufficient for B.
- B is necessary for A.
- A only if B.

If A then B. ($A \Rightarrow B$)

Alternative terminology:

- A implies B.
- Whenever A we have B.
- A is sufficient for B.
- B is necessary for A.
- A only if B.
- $B \Leftarrow A$.

If A then B. ($A \Rightarrow B$)

Alternative terminology:

- A implies B.
- Whenever A we have B.
- A is sufficient for B.
- B is necessary for A.
- A only if B.
- $B \Leftarrow A$.

Vacuous truth:

If an integer is both a perfect square and prime, then it is negative.

$A \Rightarrow B$ is only false if it is possible for A to be true but B to be false at the same time.$\rightarrow$ This is true!

An algorithmic explanation:

```
def evaluate():
    for a in Integers:
        if (a in PerfSq) and (a in Primes) ...
                          and (a > 0):
            return False

    return True
```

A if and only if B. ($A \Leftrightarrow B$)

If an integer x is even, then $x + 1$ is odd, and if $x + 1$ is odd, then x is even.

This is inconveniently long. Rather:

An integer x is even if and only if $x + 1$ is odd.

A	B	
True	True	Possible
True	False	Impossible
False	True	Impossible
False	False	Possible

Alternative terminology:

- A iff B.

A if and only if B. ($A \Leftrightarrow B$)

If an integer x is even, then $x+1$ is odd, and if $x+1$ is odd, then x is even.

This is inconveniently long. Rather:

An integer x is even if and only if $x+1$ is odd.

A	B	
True	True	Possible
True	False	Impossible
False	True	Impossible
False	False	Possible

Alternative terminology:

- A iff B.
- A is necessary and sufficient for B.

A if and only if B. ($A \Leftrightarrow B$)

If an integer x is even, then $x+1$ is odd, and if $x+1$ is odd, then x is even.

This is inconveniently long. Rather:

An integer x is even if and only if $x+1$ is odd.

A	B	
True	True	Possible
True	False	Impossible
False	True	Impossible
False	False	Possible

Alternative terminology:

- A iff B.
- A is necessary and sufficient for B.
- A is equivalent to B.

And, Or and Not

A	B	A and B
True	True	True
True	False	False
False	True	False
False	False	False

A	B	A or B
True	True	True
True	False	True
False	True	True
False	False	False

A	Not A
True	False
False	True

What theorems are called

- **Result** A modest word for a theorem.

What theorems are called

- **Result** A modest word for a theorem.
- **Fact** A very minor theorem.

What theorems are called

- **Result** A modest word for a theorem.
- **Fact** A very minor theorem.
- **Proposition** A minor theorem.

What theorems are called

- **Result** A modest word for a theorem.
- **Fact** A very minor theorem.
- **Proposition** A minor theorem.
- **Lemma** A theorem whose main purpose is to be used in the proof of a more important theorem.

What theorems are called

- **Result** A modest word for a theorem.
- **Fact** A very minor theorem.
- **Proposition** A minor theorem.
- **Lemma** A theorem whose main purpose is to be used in the proof of a more important theorem.
- **Corollary** A result with a short proof whose main step is to use a previously proved bigger theorem.

What theorems are called

- **Result** A modest word for a theorem.
- **Fact** A very minor theorem.
- **Proposition** A minor theorem.
- **Lemma** A theorem whose main purpose is to be used in the proof of a more important theorem.
- **Corollary** A result with a short proof whose main step is to use a previously proved bigger theorem.
- **Claim** Similar to a lemma but it usually appears inside the proof of a theorem to help structure it.

Outline

1 Theorems

2 Proof

What is a proof?

We create mathematical concepts via definitions and then posit assertions about them as theorems. Finally, we have to prove that our assertions are correct.

What is a proof?

We create mathematical concepts via definitions and then posit assertions about them as theorems. Finally, we have to prove that our assertions are correct.

All prime numbers are odd

What is a proof?

We create mathematical concepts via definitions and then posit assertions about them as theorems. Finally, we have to prove that our assertions are correct.

All prime numbers are odd

We cannot prove this by experimentation:

$$3, 5, 7, \cdots \qquad \text{all odd.}$$

What is a proof?

We create mathematical concepts via definitions and then posit assertions about them as theorems. Finally, we have to prove that our assertions are correct.

All prime numbers are odd

We cannot prove this by experimentation:

$$3, 5, 7, \cdots \qquad \text{all odd.}$$

Nevertheless, 2 is not odd and therefore the statement is false.

What is a proof?

Another example:

Goldbach's Conjecture

Every even integer greater than two is the sum of two primes.

What is a proof?

Another example:

Goldbach's Conjecture

Every even integer greater than two is the sum of two primes.

$$\begin{array}{cccc} 4 = 2 + 2 & 6 = 3 + 3 & 8 = 3 + 5 & 10 = 3 + 7 \\ 12 = 5 + 7 & 14 = 7 + 7 & 16 = 11 + 5 & 18 = 11 + 7 \end{array}$$

A computer can tell you that the first few billion even numbers are good too.

What is a proof?

Another example:

Goldbach's Conjecture

Every even integer greater than two is the sum of two primes.

$$4 = 2 + 2 \qquad 6 = 3 + 3 \qquad 8 = 3 + 5 \qquad 10 = 3 + 7$$
$$12 = 5 + 7 \qquad 14 = 7 + 7 \qquad 16 = 11 + 5 \qquad 18 = 11 + 7$$

A computer can tell you that the first few billion even numbers are good too.

We still do not know if we can or cannot find a larger one that would break the conjecture!

What is a proof?

A proof is an essay that incontrovertibly shows that a statement is true.

What is a proof?

A proof is an essay that incontrovertibly shows that a statement is true.

- Mathematical proofs are highly structured

What is a proof?

A proof is an essay that incontrovertibly shows that a statement is true.

- Mathematical proofs are highly structured
- They are written in a stylized manner using logical constructions.

What is a proof?

A proof is an essay that incontrovertibly shows that a statement is true.

- Mathematical proofs are highly structured
- They are written in a stylized manner using logical constructions.
- Ultimately, writing proofs is an art and you can only learn doing it well by doing it a lot.

An example

Theorem

The sum of two even integers is even.

An example

Theorem

The sum of two even integers is even.

We will use:

Definition 1

An integer is called **even** if it is divisible by two.

Definition 2

Let a and b be integers. We say that a is **divisible** by b provided there is an integer c such that $bc = a$.

Theorem

The sum of two even integers is even.

In a math paper the proof would look like this:

Proof.

We show that if x and y are even integers, then $x + y$ is an even integer.

Let x and y be even integers. Since x is even, we know by Definition 1 that $2|x$. By Definition 2, this implies that there is an integer a such that $x = 2a$. Likewise, since y is even, we have $2|y$ and therefore there is another integer b such that $y = 2b$. Observe that

$$x + y = 2a + 2b = 2(a + b).$$

This means that there is an integer $c(= a + b)$ such that $x + y = 2c$, which in turn implies $2|x + y$ which in turn implies that $x + y$ is even. $\square$

Let's break it down

1. 'We show that if x and y are even integers, then $x + y$ is an even integer.'

Let's break it down

1. 'We show that if x and y are even integers, then $x + y$ is an even integer.'

- Spells out the proposition in an *if* $-$ *then* form.

Let’s break it down

1. ’We show that if x and y are even integers, then $x + y$ is an even integer.’

- Spells out the proposition in an *if* $-$ *then* form.
- Announces the structure of the proof.

Let's break it down

1. 'We show that if x and y are even integers, then $x + y$ is an even integer.'

- Spells out the proposition in an *if* $-$ *then* form.
- Announces the structure of the proof.
- Can be considered a preamble.

Let's break it down

1. 'We show that if x and y are even integers, then $x + y$ is an even integer.'

- Spells out the proposition in an *if* $-$ *then* form.
- Announces the structure of the proof.
- Can be considered a preamble.
- Unless it serves a purpose, you can omit it. However, it is in good style to include it whenever it makes matters clearer.

Let's break it down

1. 'We show that if x and y are even integers, then $x + y$ is an even integer.'

- Spells out the proposition in an *if* $-$ *then* form.
- Announces the structure of the proof.
- Can be considered a preamble.
- Unless it serves a purpose, you can omit it. However, it is in good style to include it whenever it makes matters clearer.

2. 'Let x and y be even integers.'

Let's break it down

1. 'We show that if x and y are even integers, then $x + y$ is an even integer.'

- Spells out the proposition in an *if* $-$ *then* form.
- Announces the structure of the proof.
- Can be considered a preamble.
- Unless it serves a purpose, you can omit it. However, it is in good style to include it whenever it makes matters clearer.

2. 'Let x and y be even integers.'

- We introduce names x, y for the two integers.

Let’s break it down

1. ’We show that if x and y are even integers, then $x + y$ is an even integer.’

- Spells out the proposition in an *if* $-$ *then* form.
- Announces the structure of the proof.
- Can be considered a preamble.
- Unless it serves a purpose, you can omit it. However, it is in good style to include it whenever it makes matters clearer.

2. ’Let x and y be even integers.’

- We introduce names x, y for the two integers.
- By this we do the proof for all integers at once!

Let's break it down

3. 'Since x is even, we know by Definition 1 that $2|x$.'

Let's break it down

3. 'Since x is even, we know by Definition 1 that $2|x$.'

- We unravel the definition of even.

Let's break it down

3. 'Since x is even, we know by Definition 1 that $2|x$.'

- We unravel the definition of even.

4. 'By Definition 2, this implies that there is an integer a such that $x = 2a$.'

Let's break it down

3. 'Since x is even, we know by Definition 1 that $2|x$.'

- We unravel the definition of even.

4. 'By Definition 2, this implies that there is an integer a such that $x = 2a$.'

- We unravel the definition of divisible.

Let's break it down

3. 'Since x is even, we know by Definition 1 that $2|x$.'

- We unravel the definition of even.

4. 'By Definition 2, this implies that there is an integer a such that $x = 2a$.'

- We unravel the definition of divisible.
- A new integer comes into play, we do not know what it is as it depends on x. But we know that there is one! We denote it by a whatever it is.

Let's break it down

5. 'Likewise, since y is even, we have $2|y$ and therefore there is another integer b such that $y = 2b$.'

Let's break it down

5. 'Likewise, since y is even, we have $2|y$ and therefore there is another integer b such that $y = 2b$.'

- We do the same thing as in $3 - 4$ but this time for y. No reason to repeat the argument, we just indicate that it is the same by 'Likewise'.

Let's break it down

5. 'Likewise, since y is even, we have $2|y$ and therefore there is another integer b such that $y = 2b$.'

- We do the same thing as in $3 - 4$ but this time for y. No reason to repeat the argument, we just indicate that it is the same by 'Likewise'.

6. 'This means that there is an integer $c(= a + b)$ such that $x + y = 2c$, which in turn implies $2|x + y$'

Let's break it down

5. 'Likewise, since y is even, we have $2|y$ and therefore there is another integer b such that $y = 2b$.'

- We do the same thing as in $3 - 4$ but this time for y. No reason to repeat the argument, we just indicate that it is the same by 'Likewise'.

6. 'This means that there is an integer $c(= a + b)$ such that $x + y = 2c$, which in turn implies $2|x + y$'

- Unravel the definitions the exact same way as before but at the end of the proof!

At this point:

Proof.

We show that if x and y are even integers, then $x + y$ is an even integer.

Let x and y be even integers. Since x is even, we know by Definition 1 that $2|x$. By Definition 2, this implies that there is an integer a such that $x = 2a$. Likewise, since y is even, we have $2|y$ and therefore there is another integer b such that $y = 2b$.

there is an integer $c(= a + b)$ such that $x + y = 2c$, which in turn implies $2|x + y$ which in turn implies that $x + y$ is even. □

Proof.

We show that if x and y are even integers, then $x+y$ is an even integer.

Let x and y be even integers. Since x is even, we know by Definition 1 that $2|x$. By Definition 2, this implies that there is an integer a such that $x = 2a$. Likewise, since y is even, we have $2|y$ and therefore there is another integer b such that $y = 2b$.

there is an integer $c(= a+b)$ such that $x+y = 2c$, which in turn implies $2|x+y$ which in turn implies that $x+y$ is even. $\square$

- We make the connection between the beginning and the end.

Proof.

We show that if x and y are even integers, then $x+y$ is an even integer.

Let x and y be even integers. Since x is even, we know by Definition 1 that $2|x$. By Definition 2, this implies that there is an integer a such that $x=2a$. Likewise, since y is even, we have $2|y$ and therefore there is another integer b such that $y=2b$.

there is an integer $c(=a+b)$ such that $x+y=2c$, which in turn implies $2|x+y$ which in turn implies that $x+y$ is even. $\square$

- We make the connection between the beginning and the end.
- This is where we have to think.

Proof.

We show that if x and y are even integers, then $x + y$ is an even integer.

Let x and y be even integers. Since x is even, we know by Definition 1 that $2|x$. By Definition 2, this implies that there is an integer a such that $x = 2a$. Likewise, since y is even, we have $2|y$ and therefore there is another integer b such that $y = 2b$. Observe that

$$x + y = 2a + 2b = 2(a + b).$$

This means that there is an integer $c(= a + b)$ such that $x + y = 2c$, which in turn implies $2|x + y$ which in turn implies that $x + y$ is even. $\square$

- We make the connection between the beginning and the end.
- This is where we have to think.

Proof template

Proof template for a direct proof of an if-then theorem

1. Write the first sentence(s) of the proof by restating the hypothesis as an if-then statement. Invent suitable notation, assign letters as names to variables, etc.

Proof template

Proof template for a direct proof of an if-then theorem

1. Write the first sentence(s) of the proof by restating the hypothesis as an if-then statement. Invent suitable notation, assign letters as names to variables, etc.
2. Write the last sentence of the proof by restating the conclusion of the result.

Proof template

Proof template for a direct proof of an if-then theorem

1. Write the first sentence(s) of the proof by restating the hypothesis as an if-then statement. Invent suitable notation, assign letters as names to variables, etc.
2. Write the last sentence of the proof by restating the conclusion of the result.
3. Unravel the definitions, working forward from the beginning of the proof and backward from the end.

Proof template

Proof template for a direct proof of an if-then theorem

1. Write the first sentence(s) of the proof by restating the hypothesis as an if-then statement. Invent suitable notation, assign letters as names to variables, etc.
2. Write the last sentence of the proof by restating the conclusion of the result.
3. Unravel the definitions, working forward from the beginning of the proof and backward from the end.
4. Figure out what you know and what you need. Try to forge an argument.

Another example

Theorem

Let a, b, c be integers. If $a|b$ and $b|c$ then $a|c$.

Another example

Theorem

Let a, b, c be integers. If $a|b$ and $b|c$ then $a|c$.

This on your worksheet, give it a try now!

A more involved example

Pick a positive integer, cube it and then add it to one:

$$3^3 + 1 = 27 + 1 = 28 = 2 \cdot 14$$

$$4^3 + 1 = 64 + 1 = 65 = 5 \cdot 13$$

$$5^3 + 1 = 125 + 1 = 126 = 2 \cdot 63$$

$$6^3 + 1 = 216 + 1 = 217 = 7 \cdot 31$$

$$\vdots$$

$$x^3 + 1 = \textit{composite}?$$

A more involved example

Pick a positive integer, cube it and then add it to one:

$$3^3 + 1 = 27 + 1 = 28 = 2 \cdot 14$$
$$4^3 + 1 = 64 + 1 = 65 = 5 \cdot 13$$
$$5^3 + 1 = 125 + 1 = 126 = 2 \cdot 63$$
$$6^3 + 1 = 216 + 1 = 217 = 7 \cdot 31$$
$$\vdots$$
$$x^3 + 1 = \textit{composite}?$$

Try to formulate a theorem:

Theorem (Draft 1)

If x is an integer, then $x^3 + 1$ is composite.

A more involved example

Pick a positive integer, cube it and then add it to one:

$$3^3 + 1 = 27 + 1 = 28 = 2 \cdot 14$$
$$4^3 + 1 = 64 + 1 = 65 = 5 \cdot 13$$
$$5^3 + 1 = 125 + 1 = 126 = 2 \cdot 63$$
$$6^3 + 1 = 216 + 1 = 217 = 7 \cdot 31$$
$$\vdots$$
$$x^3 + 1 = \textit{composite}?$$

Try to formulate a theorem:

Theorem (Draft 1)

If x is an integer, then $x^3 + 1$ is composite.

Is this okay?

Theorem (Draft 1)

If x is an integer, then $x^3 + 1$ is composite.

Recall:

Definition

A positive integer a is called **composite** provided there is an integer b such that $1 < b < a$ and $b|a$.

Theorem (Draft 1)

If x is an integer, then $x^3 + 1$ is composite.

Recall:

Definition

A positive integer a is called **composite** provided there is an integer b such that $1 < b < a$ and $b|a$.

This is a problem because $x^3 + 1$ can be negative or zero!

Theorem (Draft 1)

If x is an integer, then $x^3 + 1$ is composite.

Recall:

Definition

A positive integer a is called **composite** provided there is an integer b such that $1 < b < a$ and $b|a$.

This is a problem because $x^3 + 1$ can be negative or zero!

Theorem (Draft 2)

If x is a positive integer, then $x^3 + 1$ is composite.

Theorem (Draft 1)

If x is an integer, then $x^3 + 1$ is composite.

Recall:

Definition

A positive integer a is called **composite** provided there is an integer b such that $1 < b < a$ and $b|a$.

This is a problem because $x^3 + 1$ can be negative or zero!

Theorem (Draft 2)

If x is a positive integer, then $x^3 + 1$ is composite.

But if $x = 1$ then $x^3 + 1 = 2$ which is not composite.

Theorem

Let x be an integer. If $x > 1$, then $x^3 + 1$ is composite.

Proof.

. $\square$

Theorem

Let x be an integer. If $x > 1$, then $x^3 + 1$ is composite.

Proof.

Let x be an integer and suppose $x > 1$.

we

have that $x^3 + 1$ is composite. $\square$

The statement is already if-then, no need to repeat it.

Theorem

Let x be an integer. If $x > 1$, then $x^3 + 1$ is composite.

Proof.

Let x be an integer and suppose $x > 1$.

Since is a divisor of $x^3 + 1$ and $1 <$ $< x^3 + 1$, we have that $x^3 + 1$ is composite. □

Unraveling the definition in the end.

Theorem

Let x be an integer. If $x > 1$, then $x^3 + 1$ is composite.

Proof.

Let x be an integer and suppose $x > 1$.

Since is a divisor of $x^3 + 1$ and $1 < \quad < x^3 + 1$, we have that $x^3 + 1$ is composite. □

Unraveling the definition in the end.

What should be the right divisor?

Since is a divisor of $x^3 + 1$ and $1 < \quad < x^3 + 1$, we have that $x^3 + 1$ is composite.

Since is a divisor of $x^3 + 1$ and $1 < \quad < x^3 + 1$, we have that $x^3 + 1$ is composite.

Recall:

Definition

Let a and b integers. If $a|b$ and $1 < a < b$ then a is called a **factor** of b.

Since is a divisor of $x^3 + 1$ and $1 < \qquad < x^3 + 1$, we have that $x^3 + 1$ is composite.

Recall:

Definition

Let a and b integers. If $a|b$ and $1 < a < b$ then a is called a **factor** of b.

We need to find a factor!

Since is a divisor of $x^3 + 1$ and $1 < \quad < x^3 + 1$, we have that $x^3 + 1$ is composite.

Recall:

Definition

Let a and b integers. If $a|b$ and $1 < a < b$ then a is called a **factor** of b.

We need to find a factor!

$$x^3 + 1 = (x + 1)(x^2 - x + 1)$$

and so $x + 1$ and $x^2 - x + 1$ are both factors of $x^3 + 1$ as they are both integers (since x is an integer).

Theorem

Let x be an integer. If $x > 1$, then $x^3 + 1$ is composite.

Proof.

Let x be an integer and suppose $x > 1$. Note that $x^3 + 1 = (x+1)(x^2 - x + 1)$. Because x is an integer, both $x + 1$ and $x^2 - x + 1$ are integers. Therefore $(x+1) | (x^3 + 1)$.

Since $x + 1$ is a divisor of $x^3 + 1$ and $1 < \quad < x^3 + 1$, we have that $x^3 + 1$ is composite. □

Theorem

Let x be an integer. If $x > 1$, then $x^3 + 1$ is composite.

Proof.

Let x be an integer and suppose $x > 1$. Note that $x^3 + 1 = (x + 1)(x^2 - x + 1)$. Because x is an integer, both $x + 1$ and $x^2 - x + 1$ are integers. Therefore $(x + 1) | (x^3 + 1)$.

Since $x + 1$ is a divisor of $x^3 + 1$ and $1 <$ $< x^3 + 1$, we have that $x^3 + 1$ is composite. □

We are not done yet, as we still need to show that $x + 1$ 'fits into the gap'.

We need

$$1 < x + 1 < x^3 + 1$$

We need

$$1 < x + 1 < x^3 + 1$$

First inequality:

$$x > 1 \qquad \rightarrow \qquad x + 1 > 1 + 1 = 2 > 1$$

We need

$$1 < x + 1 < x^3 + 1$$

First inequality:

$$x > 1 \qquad \to \qquad x + 1 > 1 + 1 = 2 > 1$$

The second inequality:

$$\begin{aligned} x > 1 \qquad &\to \qquad x^2 > x > 1 && \text{(multiplying by } x\text{)} \\ &\to \qquad x^3 > x && \text{(multiplying by } x\text{)} \\ &\to \qquad x^3 + 1 > x + 1 && \text{(adding } 1\text{)} \end{aligned}$$

Theorem

Let x be an integer. If $x > 1$, then $x^3 + 1$ is composite.

Proof.

Let x be an integer and suppose $x > 1$. Note that $x^3 + 1 = (x + 1)(x^2 - x + 1)$. Because x is an integer, both $x + 1$ and $x^2 - x + 1$ are integers. Therefore $(x + 1) | (x^3 + 1)$.

Since $x > 1$, we have $x + 1 > 1 + 1 = 2 > 1$.

Also $x > 1$ implies $x^2 > x$, and since $x > 1$, we have $x^2 > 1$. Multiplying both sides by x again yields $x^3 > x$. Adding 1 to both sides gives $x^3 + 1 > x + 1$.

Thus $x + 1$ is an integer with $1 < x + 1 < x^3 + 1$.

Since $x + 1$ is a divisor of $x^3 + 1$ and $1 < x + 1 < x^3 + 1$, we have that $x^3 + 1$ is composite. $\square$

If-and-only-if Theorems

Direct proof of an if-and-only-if theorem

To prove a statement of the form '*A* iff *B*',

- ($\Rightarrow$) Prove 'If *A*, then *B*'.
- ($\Leftarrow$) Prove 'If *B*, then *A*'.

If-and-only-if Theorems

Direct proof of an if-and-only-if theorem

To prove a statement of the form 'A iff B',

- ($\Rightarrow$) Prove 'If A, then B'.
- ($\Leftarrow$) Prove 'If B, then A'.

Theorem

Let x be an integer. Then x is even if and only if $x + 1$ is odd.

If-and-only-if Theorems

Direct proof of an if-and-only-if theorem

To prove a statement of the form 'A iff B',

- ($\Rightarrow$) Prove 'If A, then B'.
- ($\Leftarrow$) Prove 'If B, then A'.

Theorem

Let x be an integer. Then x is even if and only if $x + 1$ is odd.

Proof.

Let x be an integer.
($\Rightarrow$) Suppose x is even, $\ldots$ Therefore $x + 1$ is odd.
($\Leftarrow$) Suppose $x + 1$ is odd, $\ldots$ Therefore x is even. $\square$

Now prove the if-then substatements as before. (Worksheet)