Contrapositive Proof

MAT231

Transition to Higher Mathematics

Fall 2014

Outline

A Simple Proposition

Consider

Proposition

Suppose $n \in \mathbb{Z}$. If $3 \nmid n^2$, then $3 \nmid n$.

How might we start a proof of this statement? Since it is of the form "if P, then Q" we might try to start with $3 \nmid n^2$:

- Try $n^2 = 3q + r$ for some $q, r \in \mathbb{Z}$ with $r = 1$ or $r = 2$.
- We would need to use cases, and even then it's not clear how we'd proceed given that we started with n^2.

Contrapositive Statements

Recall that a statement and it's *contrapositive* are logically equivalent.

P	Q	$P \Rightarrow Q$	$\sim Q$	$\sim P$	$\sim Q \Rightarrow \sim P$
T	T	**T**	F	F	**T**
T	F	**F**	T	F	**F**
F	T	**T**	F	T	**T**
F	F	**T**	T	T	**T**

This means that if we prove $\sim Q \Rightarrow \sim P$, we've also proven $P \Rightarrow Q$.

This is called **contrapositive proof**. It proves $P \Rightarrow Q$ by a direct proof of the contrapositive statement $\sim Q \Rightarrow \sim P$.

Contrapositive Proof Example

Proposition

Suppose $n \in \mathbb{Z}$. If $3 \nmid n^2$, then $3 \nmid n$.

Proof.

(Contrapositive) Let integer n be given. If $3|n$ then $n = 3a$ for some $a \in \mathbb{Z}$. Squaring, we have

$$n^2 = (3a)^2 = 3(3a^2) = 3b$$

where $b = 3a^2$. By the closure property, we know b is an integer, so we see that $3|n^2$. The proves the contrapositive of the original proposition, and so completes the proof. $\square$

Congruence of Integers

Definition

Given integers a and b and an $n \in \mathbb{N}$, we say that a and b are **congruent modulo** n if $n|(a-b)$. This is written as

$$a \equiv b \pmod{n}.$$

Note: Think of this as

"a is equivalent to b (Pssst, as long as we are using modulo n)."

In other words, the "(mod n)" qualifies the entire statement, not just b. In particular, this statement does **not** say that a is some how related to something called b mod n.

The Modulo Operator

The Division Algorithm asserts that, given any integers a, b, q, r with $b \neq 0$ and $0 \leq r < b$, we can write $a = bq + r$.

- If we work only with integer division (i.e., we compute the quotient and drop the remainder), then

$$q = a/b.$$

- We can define an operator to compute the remainder. We'll call it "mod." Thus

$$r = a \bmod b.$$

It turns out that the definition of congruence means that $a \equiv b \pmod{n}$ if and only if $a \bmod n = b \bmod n$.

That is, both a and b have the same remainder when divided by n.

The Modulo Operator: Proof Part 1

Proposition

Suppose $a, b \in \mathbb{Z}$ *and* $n \in \mathbb{N}$. *If* a *mod* $n = b$ *mod* n, *then* $a \equiv b \pmod{n}$.

The Modulo Operator: Proof Part 1

Proposition

Suppose $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$. If $a \bmod n = b \bmod n$, then $a \equiv b \pmod{n}$.

Proof.

Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$ be given. Because both a and b have the same remainder when divided by n, by the division algorithm $q_1, q_2, r \in \mathbb{Z}$ exist such that $0 \leq r < n$ and

$$a = nq_1 + r \qquad \text{and} \qquad b = nq_2 + r$$

Forming $a - b$ we find

$$a - b = (nq_1 + r) - (nq_2 + r) = n(q_1 - q_2).$$

This shows $a - b$ is a multiple of n so $n|(a - b)$ and therefore $a \equiv b \pmod{n}$. □

The Modulo Operator: Proof Part 2

Proposition

Suppose $a, b \in \mathbb{Z}$ *and* $n \in \mathbb{N}$. *If* $a \equiv b \ (mod\ n)$, *then* $a \ mod\ n = b \ mod\ n$.

The Modulo Operator: Proof Part 2

Proposition

Suppose $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$. If $a \equiv b \pmod{n}$, then $a \bmod n = b \bmod n$.

Proof.

Let $a, b \in \mathbb{Z}$ and $n \in \mathbb{N}$ be given. By the division algorithm, $q_1, q_2, r_1, r_2 \in \mathbb{Z}$ exist such that $0 \leq r_1, r_2 < n$ and

$$a = nq_1 + r_1 \qquad \text{and} \qquad b = nq_2 + r_2$$

where r_1 and r_2 are the remainders that result when a and b are divided by n, respectively. If $a \equiv b \pmod{n}$, then $n|(a-b)$. This is only possible if $r_1 = r_2$ since $a - b = n(q_1 - q_2) + (r_1 - r_2)$ and the remainder of $a - b$ divided by n must be zero. Therefore, a and b must have the same remainder when divided by n, so $a \bmod n = b \bmod n$. $\square$

Examples of Congruence

- $7 \equiv 3 \pmod 2$ since $7 - 3 = 4$ is a multiple of 2.
- $4 \equiv 19 \pmod 5$ since $4 - 19 = -15$ and $5 | (-15)$.
- $4 \equiv -1 \pmod 5$ since $4 - (-1) = 5$ and $5 | 5$.
- $13 \not\equiv 8 \pmod 3$ since $13 - 8 = 5$ and $3 \nmid 5$.

Sometimes working with modular arithmetic is referred to as *clock arithmetic* since we are used to problems like

Example

It is now 45 minutes past the hour. What time will it be in 25 minutes?

$$(45 + 25) \bmod 60 = 70 \bmod 60 = 10$$

so it will be 10 minutes past the (next) hour.

A Useful Lemma

Lemma

For any $m \in \mathbb{R}$ *and* $p \in \mathbb{N}$

$$m^p - 1 = (m-1)(m^{p-1} + m^{p-2} + \cdots + m^2 + m + 1)$$

Proof.

Let $m \in \mathbb{R}$ and $p \in \mathbb{N}$ be given. Then

$$\begin{aligned}
&(m-1)(m^{p-1} + m^{p-2} + \cdots + m^2 + m + 1) \\
&\qquad = (m^p + m^{p-1} + \cdots + m^2 + m) - (m^{p-1} + m^{p-2} + \cdots + m + 1) \\
&\qquad = m^p + (m^{p-1} - m^{p-1}) + (m^{p-2} - m^{p-2}) + \cdots + (m - m) - 1 \\
&\qquad = m^p - 1.
\end{aligned}$$

$\square$

(This is an example of a **telescoping sum**.)

Proof Example

Proposition

If $n \in \mathbb{N}$ *and* $2^n - 1$ *is prime, then* n *is prime.*

Proof.

(Contrapositive) Suppose $n \in \mathbb{N}$ is composite with factors $a > 1$ and $b > 1$. Then

$$2^n - 1 = 2^{ab} - 1 = (2^b)^a - 1.$$

Using our lemma with $m = 2^b$ and $p = a$ we have

$$2^n - 1 = (2^b - 1)(2^{ab-b} + 2^{ab-2b} + \cdots + 2^{ab-(a-1)b} + 2^{ab-ab}).$$

Thus $2^n - 1$ is composite. $\square$

Notice that we could not have done this if n was prime because then $a = n$ and $b = 1$ so $2^b - 1 = 2 - 1 = 1$, which would mean one of the factors in our result was 1.

Mathematical Writing

The following list comes from our text. Please make every effort to follow these suggestions. The list ends with helpful hints on using words like *since, because, as for, so*, and *thus, hence, therefore, consequently*.

1. Never begin a sentence with a mathematical symbol.

Mathematical Writing

The following list comes from our text. Please make every effort to follow these suggestions. The list ends with helpful hints on using words like *since, because, as for, so*, and *thus, hence, therefore, consequently*.

1. Never begin a sentence with a mathematical symbol.
2. Use correct punctuation. For example, end each sentence with a period, even if it ends with a stand-alone equation.

Mathematical Writing

The following list comes from our text. Please make every effort to follow these suggestions. The list ends with helpful hints on using words like *since, because, as for, so*, and *thus, hence, therefore, consequently*.

1. Never begin a sentence with a mathematical symbol.
2. Use correct punctuation. For example, end each sentence with a period, even if it ends with a stand-alone equation.
3. Separate mathematical symbols and expressions with words.

Mathematical Writing

The following list comes from our text. Please make every effort to follow these suggestions. The list ends with helpful hints on using words like *since, because, as for, so*, and *thus, hence, therefore, consequently*.

1. Never begin a sentence with a mathematical symbol.
2. Use correct punctuation. For example, end each sentence with a period, even if it ends with a stand-alone equation.
3. Separate mathematical symbols and expressions with words.
4. Avoid misuse of symbols.

Mathematical Writing

The following list comes from our text. Please make every effort to follow these suggestions. The list ends with helpful hints on using words like *since, because, as for, so*, and *thus, hence, therefore, consequently*.

1. Never begin a sentence with a mathematical symbol.
2. Use correct punctuation. For example, end each sentence with a period, even if it ends with a stand-alone equation.
3. Separate mathematical symbols and expressions with words.
4. Avoid misuse of symbols.
5. Avoid using unnecessary symbols.

Mathematical Writing

The following list comes from our text. Please make every effort to follow these suggestions. The list ends with helpful hints on using words like *since, because, as for, so*, and *thus, hence, therefore, consequently*.

1. Never begin a sentence with a mathematical symbol.
2. Use correct punctuation. For example, end each sentence with a period, even if it ends with a stand-alone equation.
3. Separate mathematical symbols and expressions with words.
4. Avoid misuse of symbols.
5. Avoid using unnecessary symbols.
6. Use the first person plural.

Mathematical Writing

The following list comes from our text. Please make every effort to follow these suggestions. The list ends with helpful hints on using words like *since, because, as for, so*, and *thus, hence, therefore, consequently*.

1. Never begin a sentence with a mathematical symbol.
2. Use correct punctuation. For example, end each sentence with a period, even if it ends with a stand-alone equation.
3. Separate mathematical symbols and expressions with words.
4. Avoid misuse of symbols.
5. Avoid using unnecessary symbols.
6. Use the first person plural.
7. Use the active voice.

Mathematical Writing

The following list comes from our text. Please make every effort to follow these suggestions. The list ends with helpful hints on using words like *since, because, as for, so*, and *thus, hence, therefore, consequently*.

1. Never begin a sentence with a mathematical symbol.
2. Use correct punctuation. For example, end each sentence with a period, even if it ends with a stand-alone equation.
3. Separate mathematical symbols and expressions with words.
4. Avoid misuse of symbols.
5. Avoid using unnecessary symbols.
6. Use the first person plural.
7. Use the active voice.
8. Explain each new symbol.

Mathematical Writing

The following list comes from our text. Please make every effort to follow these suggestions. The list ends with helpful hints on using words like *since, because, as for, so*, and *thus, hence, therefore, consequently*.

1. Never begin a sentence with a mathematical symbol.
2. Use correct punctuation. For example, end each sentence with a period, even if it ends with a stand-alone equation.
3. Separate mathematical symbols and expressions with words.
4. Avoid misuse of symbols.
5. Avoid using unnecessary symbols.
6. Use the first person plural.
7. Use the active voice.
8. Explain each new symbol.
9. Watch out for "it."