# Math 325K - Lecture 7
# Section 4.1 Direct proof and counterexample I

Bo Lin

September 20th, 2018

# Outline

- Basic definitions in number theory.
- Prove and disprove universal statements.
- Prove and disprove existential statements.
- Tips and common mistakes.

# Application of logic in proofs

**Remark**

*Essentially, proofs are sound arguments whose conclusion is the statement we need to prove. So when writing a proof, we need to make sure that the argument is valid, and all premises are true.*

# Application of logic in proofs

**Remark**

*Essentially, proofs are sound arguments whose conclusion is the statement we need to prove. So when writing a proof, we need to make sure that the argument is valid, and all premises are true.*

**Remark**

*The main reason that we introduced logic is to write proofs. The theory of logic tells us what are valid argument forms and how to draw new conclusions from the premises we already have, until we reach the final conclusion.*

# Properties of equality

## Definition

*An* **equivalence relation** $R$ *is a relation defined on* $D \times D$ *(where* $D$ *is a set) satifying the following three properties:*

- *(reflexive)* $\forall x \in D$*, we have* $R(x, x)$*;*
- *(commutative)* $\forall x, y \in D$*, if* $R(x, y)$*, then* $R(y, x)$*;*
- *(transitive)* $\forall x, y, z \in D$*, if* $R(x, y)$ *and* $R(y, z)$*, then* $R(x, z)$*.*

# Properties of equality

## Definition

*An* **equivalence relation** $R$ *is a relation defined on* $D \times D$ *(where* $D$ *is a set) satifying the following three properties:*

- *(reflexive)* $\forall x \in D$*, we have* $R(x, x)$*;*
- *(commutative)* $\forall x, y \in D$*, if* $R(x, y)$*, then* $R(y, x)$*;*
- *(transitive)* $\forall x, y, z \in D$*, if* $R(x, y)$ *and* $R(y, z)$*, then* $R(x, z)$*.*

## Remark

*In mathematics, a lot of relations are equivalence relations. For example, equality* $=$*; logical equivalence* $\equiv$*; congruence of integers modulo* $m \equiv \pmod{m}$*.*

# Even and odd integers

## Definition

*An integer $n$ is even if and only if $n$ equals twice some integer. An integer $n$ is* **odd** *if and only if $n$ equals twice some integer plus $1$. In symbols,*

$$n \text{ is even } \Leftrightarrow \exists k \in \mathbb{Z} \text{ such that } n = 2k.$$

$$n \text{ is odd } \Leftrightarrow \exists k \in \mathbb{Z} \text{ such that } n = 2k + 1.$$

# Prime and composite numbers

## Definition

*An integer $n$ is prime if and only if $n > 1$ and for all positive integers $r$ and $s$, if $n = rs$, then either $r$ or $s$ equals $n$. An integer $n$ is composite if and only if $n > 1$ and $n = rs$ for some integers $r$ and $s$ with $1 < r < n$ and $1 < s < n$.*

# Prime and composite numbers

## Definition

*An integer $n$ is prime if and only if $n > 1$ and for all positive integers $r$ and $s$, if $n = rs$, then either $r$ or $s$ equals $n$. An integer $n$ is composite if and only if $n > 1$ and $n = rs$ for some integers $r$ and $s$ with $1 < r < n$ and $1 < s < n$.*

## Remark

*Note that $1$ is neither prime nor composite. Prime numbers are the central object in the study of number theory and there are still a lot unsolved problems (for example the Twin Prime Conjecture) related to prime numbers.*

# Example: quick questions

## Example

(a) *if* $a$ *is an even integer, is* $a^2$ *even or odd?*

(b) *if* $a$ *and* $b$ *are integers, is* $6a + 4b + 3$ *even or odd?*

(c) *is* $17$ *a prime number?*

# Example: quick questions

## Example

(a) *if $a$ is an even integer, is $a^2$ even or odd?*

(b) *if $a$ and $b$ are integers, is $6a + 4b + 3$ even or odd?*

(c) *is $17$ a prime number?*

## Solution

*(a) Suppose $a = 2k$ for some integer $k$, then $a^2 = (2k)^2 = 2 \cdot 2k^2$ is even too.*

# Example: quick questions

## Example

(a) *if* $a$ *is an even integer, is* $a^2$ *even or odd?*

(b) *if* $a$ *and* $b$ *are integers, is* $6a + 4b + 3$ *even or odd?*

(c) *is* $17$ *a prime number?*

## Solution

*(a) Suppose* $a = 2k$ *for some integer* $k$*, then* $a^2 = (2k)^2 = 2 \cdot 2k^2$ *is even too.*

*(b) Note that* $6a + 4b + 3 = 2(3a + 2b + 1) + 1$*, by definition it is odd.*

# Example: quick questions

## Example

(a) *if* $a$ *is an even integer, is* $a^2$ *even or odd?*

(b) *if* $a$ *and* $b$ *are integers, is* $6a + 4b + 3$ *even or odd?*

(c) *is* $17$ *a prime number?*

## Solution

*(a) Suppose* $a = 2k$ *for some integer* $k$*, then* $a^2 = (2k)^2 = 2 \cdot 2k^2$ *is even too.*

*(b) Note that* $6a + 4b + 3 = 2(3a + 2b + 1) + 1$*, by definition it is odd.*

*(c) The only way to write* $17$ *as the product of two unordered positive integers is* $17 = 17 \cdot 1$*, by definition* $17$ *is a prime number.*

# Disproof by counterexamples

Suppose we have a universal statement $\forall x \in D, P(x)$, where $P$ is a predicate and $D$ is its domain. In order to disprove (justify that it is false) it, it suffices to find one particular element $y \in D$ such that $P(y)$ is false. Recall that such a $y$ is called a counterexample. And once $P(y)$ is shown to be false, the disproof is done.

# Disproof by counterexamples

Suppose we have a universal statement $\forall x \in D, P(x)$, where $P$ is a predicate and $D$ is its domain. In order to disprove (justify that it is false) it, it suffices to find one particular element $y \in D$ such that $P(y)$ is false. Recall that such a $y$ is called a counterexample. And once $P(y)$ is showen to be false, the disproof is done.

**Remark**

*A disproof by counterexample is usually short. In general, we do not need to write the way how we found the counterexample. We only need to include two things in the disproof: $y \in D$ and $P(y)$ is false.*

# Example: find counterexamples

## Example

*Find a counterexample for each of the following universal statements:*

(a) *The sum of two prime numbers is always a composite number.*

(b) *For every even number $n$, $\frac{n}{2}$ is an odd number.*

(c) *For all real numbers $a$ and $b$, if $a^2 = b^2$, then $a = b$.*

# Example: find counterexamples

## Example

*Find a counterexample for each of the following universal statements:*

(a) *The sum of two prime numbers is always a composite number.*

(b) *For every even number $n$, $\frac{n}{2}$ is an odd number.*

(c) *For all real numbers $a$ and $b$, if $a^2 = b^2$, then $a = b$.*

## Solution

*(a) if both prime numbers are odd, it is true. But $2 + 3 = 5$ and $2, 3, 5$ are all prime, so the pair of $2$ and $3$ is a counterexample.*

# Example: find counterexamples

## Example

*Find a counterexample for each of the following universal statements:*

(a) *The sum of two prime numbers is always a composite number.*

(b) *For every even number $n$, $\frac{n}{2}$ is an odd number.*

(c) *For all real numbers $a$ and $b$, if $a^2 = b^2$, then $a = b$.*

## Solution

*(a) if both prime numbers are odd, it is true. But $2 + 3 = 5$ and $2, 3, 5$ are all prime, so the pair of $2$ and $3$ is a counterexample.*
*(b) $4$ is even and $\frac{4}{2} = 2$ is still even, so $n = 4$ is a counterexample.*

# Example: find counterexamples

## Example

*Find a counterexample for each of the following universal statements:*

(a) *The sum of two prime numbers is always a composite number.*

(b) *For every even number $n$, $\frac{n}{2}$ is an odd number.*

(c) *For all real numbers $a$ and $b$, if $a^2 = b^2$, then $a = b$.*

## Solution

*(a) if both prime numbers are odd, it is true. But $2 + 3 = 5$ and $2, 3, 5$ are all prime, so the pair of $2$ and $3$ is a counterexample.*
*(b) $4$ is even and $\frac{4}{2} = 2$ is still even, so $n = 4$ is a counterexample.*
*(c) Let $a = 1$ and $b = -1$, the square of both numbers is $1$ while $a \neq b$. So $(a, b) = (1, -1)$ is a counterexample.*

# The method of exhaustion

In general it is more challenging to show that a universal statement is true. When the domain is finite, we can apply the method of exhaustion - check that the predicate is true for all elements in the domain.

# The method of exhaustion

In general it is more challenging to show that a universal statement is true. When the domain is finite, we can apply the method of exhaustion - check that the predicate is true for all elements in the domain.

**Remark**

*This is the most straightforward method, while even if the domain is finite, if the cardinality is too big, it is still not a good method.*

# The method of direct proof

A more efficient method would be generalizing from the generic particular: to show that every element of the domain satisfies a certain property, suppose $x$ is a particular but arbitrarily chosen element of the domain, and show that $x$ satisfies the property.

# The method of direct proof

A more efficient method would be generalizing from the generic particular: to show that every element of the domain satisfies a certain property, suppose $x$ is a particular but arbitrarily chosen element of the domain, and show that $x$ satisfies the property.

**Remark**

*When the predicate is conditional (like $P(x) \to Q(x)$), we can apply the method of direct proof: first, write the statement as "$\forall x \in D, P(x) \to Q(x)$"; second, suppose $x$ is particular but arbitrarily chosen element of $D$ for which $P(x)$ is true; finally, show that $Q(x)$ is true.*

# Example: a direct proof

**Proposition**

*The sum of two even numbers is still an even number.*

# Example: a direct proof

**Proposition**

*The sum of two even numbers is still an even number.*

**Remark**

*We can rewrite the statement as follows: let $E$ be the set of even numbers,*

$$\forall x \in E, \forall y \in E, x + y \in E.$$

*So we may choose $x$ and $y$ as two particular elements in $E$, and it suffices to show that $x + y$ is also in $E$. The last step is essential and requires the use of our premises.*

# Example: a direct proof

**Proof.**

Suppose $x$ and $y$ are even numbers. By definition, there exists an integer $r$ such that $x = 2r$ and an integer $s$ such that $y = 2s$. Then $x + y = 2r + 2s$. So it suffices to show that $2r + 2s$ is even. What do we know about $r$ and $s$? The only information is that they are integers. Fortunately it is enough:

$$2r + 2s = 2 \cdot (r + s).$$

Since $r$ and $s$ are integers, so is $r + s$. By definition, $2 \cdot (r + s)$ is even, so is $x + y$. This finishes a direct proof of our proposition. □

# Example: a direct proof

**Proof.**

Suppose $x$ and $y$ are even numbers. By definition, there exists an integer $r$ such that $x = 2r$ and an integer $s$ such that $y = 2s$. Then $x + y = 2r + 2s$. So it suffices to show that $2r + 2s$ is even. What do we know about $r$ and $s$? The only information is that they are integers. Fortunately it is enough:

$$2r + 2s = 2 \cdot (r + s).$$

Since $r$ and $s$ are integers, so is $r + s$. By definition, $2 \cdot (r + s)$ is even, so is $x + y$. This finishes a direct proof of our proposition. □

# Proving existential statements

Recall that one example is enough to prove an existential statement "$\exists x \in D$ such that $P(x)$": simply find a particular element $y$ in the domain $D$ such that $P(y)$ is true.

# Proving existential statements

Recall that one example is enough to prove an existential statement "$\exists x \in D$ such that $P(x)$": simply find a particular element $y$ in the domain $D$ such that $P(y)$ is true.

**Remark**

*When writing such a proof, we need to demonstrate two things: $y \in D$ and $P(y)$ is true.*

# Constructive versus nonconstructive proofs

There is a dichotomy between the proofs of existential statements: constructive versus nonconstructive. A **constructive proof** explicitly presents such an element $y \in D$ such that $P(y)$ is true, or presents an algorithm to find such an element.

# Constructive versus nonconstructive proofs

There is a dichotomy between the proofs of existential statements: constructive versus nonconstructive. A **constructive proof** explicitly presents such an element $y \in D$ such that $P(y)$ is true, or presents an algorithm to find such an element.
In comparison, a **nonconstructive proof** is indirect and it usually justifies the existential statement in one of the following ways: show that it is deduced from an axiom or a theorem/proposition we already got; show that from the negation of our existential statement we can deduce a contradiction.

# Constructive versus nonconstructive proofs

There is a dichotomy between the proofs of existential statements: constructive versus nonconstructive. A **constructive proof** explicitly presents such an element $y \in D$ such that $P(y)$ is true, or presents an algorithm to find such an element.
In comparison, a **nonconstructive proof** is indirect and it usually justifies the existential statement in one of the following ways: show that it is deduced from an axiom or a theorem/proposition we already got; show that from the negation of our existential statement we can deduce a contradiction.

**Remark**

*Apparently we prefer constructive proofs, while sometimes it is very hard to find one.*

# Example: proof of existential statements

## Example

*Prove that there is a positive integer $n$ such that both $n$ and $n+6$ are prime numbers.*

# Example: proof of existential statements

## Example

*Prove that there is a positive integer $n$ such that both $n$ and $n+6$ are prime numbers.*

## Proof.

It suffices to find one such $n$. We begin with the smallest prime numbers $2, 3, 5, 7, \cdots$. Plus $6$, we get $8, 9, 11, 13, \cdots$. Since $11$ is a prime number, $n = 5$ is an example, and we are done. $\square$

# Example: proof of existential statements

## Example

*Prove that there is a positive integer $n$ such that both $n$ and $n+6$ are prime numbers.*

## Proof.

It suffices to find one such $n$. We begin with the smallest prime numbers $2, 3, 5, 7, \cdots$. Plus $6$, we get $8, 9, 11, 13, \cdots$. Since $11$ is a prime number, $n = 5$ is an example, and we are done. $\square$

## Remark

*It is possible that there are more than one eligible example in the domain, and all these examples lead to correct proofs.*

# Disprove existential statements

Always keep in mind that showing that a statement is true is the same as showing that its negation is false. The negation of an existential statement is a universal statement. So we can apply the methods introduced above: exhaustion and direct proof.

# Disprove existential statements

Always keep in mind that showing that a statement is true is the same as showing that its negation is false. The negation of an existential statement is a universal statement. So we can apply the methods introduced above: exhaustion and direct proof.

**Remark**

*When taking the negation, make sure that all quantifiers and the predicates are all negated.*

# Example: disprove an existential statement

## Example

*Disprove the statement "there is a positive integer $n$ such that $n(n+1)$ is odd".*

# Example: disprove an existential statement

## Example

*Disprove the statement "there is a positive integer $n$ such that $n(n+1)$ is odd".*

## Proof.

We justify its negation "for all positive integers $n$, $n(n+1)$ is even". Let $n$ be an arbitrary positive integer. If $n$ is even, then there is an integer $k$ such that $n = 2k$. So $n(n+1) = 2k(2k+1) = 2 \cdot k(2k+1)$ is even. If $n$ is odd, then there is an integer $k$ such that $n = 2k+1$. So $n(n+1) = (2k+1)(2k+2) = 2 \cdot (2k+1)(k+1)$ is even too. Since the integer $n$ is either even or odd, by division into cases, we draw the conclusion that $n(n+1)$ is even. □

# Tips of writing proofs

- Clearly mark the beginning of your proof with the word "Proof".

# Tips of writing proofs

- Clearly mark the beginning of your proof with the word "Proof".
- Make your proof self-contained. In particular, clearly define all symbols introduced by yourselves.

# Tips of writing proofs

- Clearly mark the beginning of your proof with the word "Proof".
- Make your proof self-contained. In particular, clearly define all symbols introduced by yourselves.
- Write complete, grammatically correct sentences in your proof.

# Tips of writing proofs

- Clearly mark the beginning of your proof with the word "Proof".
- Make your proof self-contained. In particular, clearly define all symbols introduced by yourselves.
- Write complete, grammatically correct sentences in your proof.
- Make the status of statements clear (what are already justified, what are going to be justified).

# Tips of writing proofs

- Clearly mark the beginning of your proof with the word "Proof".
- Make your proof self-contained. In particular, clearly define all symbols introduced by yourselves.
- Write complete, grammatically correct sentences in your proof.
- Make the status of statements clear (what are already justified, what are going to be justified).
- Give a reason for each assertion in your proof.

# Tips of writing proofs

- Clearly mark the beginning of your proof with the word "Proof".
- Make your proof self-contained. In particular, clearly define all symbols introduced by yourselves.
- Write complete, grammatically correct sentences in your proof.
- Make the status of statements clear (what are already justified, what are going to be justified).
- Give a reason for each assertion in your proof.
- Display equations and inequalities if necessary.

# Tips of writing proofs

- Clearly mark the beginning of your proof with the word "Proof".
- Make your proof self-contained. In particular, clearly define all symbols introduced by yourselves.
- Write complete, grammatically correct sentences in your proof.
- Make the status of statements clear (what are already justified, what are going to be justified).
- Give a reason for each assertion in your proof.
- Display equations and inequalities if necessary.

# Getting proofs started

Roughly speaking, writing a proof is like building a bridge between the premises and the conclusion. As a result, there are multiple possible approaches. We can start from the side of premises, to draw new conclusions and get closer to the other end; or we can also start from the side of the conclusion, to figure out another statement that implies the conclusion, and regard this statement as a new target conclusion. In fact we usually take both approaches together. Just like building a bridge, as long as both parts do meet somewhere in the middle, the construction is done.

# Getting proofs started

Roughly speaking, writing a proof is like building a bridge between the premises and the conclusion. As a result, there are multiple possible approaches. We can start from the side of premises, to draw new conclusions and get closer to the other end; or we can also start from the side of the conclusion, to figure out another statement that implies the conclusion, and regard this statement as a new target conclusion. In fact we usually take both approaches together. Just like building a bridge, as long as both parts do meet somewhere in the middle, the construction is done.

**Remark**

*No matter which approach you take, always keep in mind the roles of all statements appeared - whether they are new conclusions deduced from premises, or they can imply and conclusion and thus they are new target conclusions.*

# Common mistakes to avoid

There are several common mistakes in writing proofs.

- Justifying a universal statement from examples.

# Common mistakes to avoid

There are several common mistakes in writing proofs.

- Justifying a universal statement from examples.
- Using the same symbol to mean different things.

# Common mistakes to avoid

There are several common mistakes in writing proofs.

- Justifying a universal statement from examples.
- Using the same symbol to mean different things.
- Assuming the conclusion and thus result in circular reasoning.

# Common mistakes to avoid

There are several common mistakes in writing proofs.

- Justifying a universal statement from examples.
- Using the same symbol to mean different things.
- Assuming the conclusion and thus result in circular reasoning.
- Confusion between what is known and what is going to be shown.

# Common mistakes to avoid

There are several common mistakes in writing proofs.

- Justifying a universal statement from examples.
- Using the same symbol to mean different things.
- Assuming the conclusion and thus result in circular reasoning.
- Confusion between what is known and what is going to be shown.
- Misuse of "any" (for $\forall$) and "some" (for $\exists$).

# Example: find the flaw in proofs

## Example

*Find the flaw in the following proof of the statement "any two odd numbers are equal":*

1. *Let $a$ and $b$ be two arbitrary odd numbers.*
2. *By definition, there exists an integer $k$ such that $a = 2k + 1$.*
3. *By definition, there exists an integer $k$ such that $b = 2k + 1$.*
4. *Then $a = 2k + 1 = b$.*

# Example: find the flaw in proofs

## Example

*Find the flaw in the following proof of the statement "any two odd numbers are equal":*

1. *Let $a$ and $b$ be two arbitrary odd numbers.*
2. *By definition, there exists an integer $k$ such that $a = 2k + 1$.*
3. *By definition, there exists an integer $k$ such that $b = 2k + 1$.*
4. *Then $a = 2k + 1 = b$.*

## Solution

*The integer $k$ depends on the choice of $a$ and $b$. Given that $k$ is already used in (2), we cannot use it in (3) again. The flaw is in (3).*

# Example: find the flaw in proofs

## Example

*Find the flaw in the following proof of the statement "for all positive integers $k$, $k^2 + 2k + 1$ is a composite number":*

1. *Let $k$ be a positive integer.*
2. *If $k^2 + 2k + 1$ is a composite number, by definition there exist positive integers $r$ and $s$ such that $rs = k^2 + 2k + 1$ and*

$$1 < r < k^2 + 2k + 1, 1 < s < k^2 + 2k + 1.$$

3. *Since $k^2 + 2k + 1$ is the product of $r$ and $s$ and $r, s$ are strictly between $1$ and $k^2 + 2k + 1$, by definition $k^2 + 2k + 1$ is a composite number.*

# Example: find the flaw in proofs

## Solution

*Here in (2), the existence of $r, s$ implies our conclusion, so we need to demonstrate this new statement. But in (3) we simply reasoned from this statement, so we did not actually prove it.*

# Example: find the flaw in proofs

## Example

*Find the flaw in the following proof of the same statement in previous example:*

1. *Let* $k = 3$ *be a positive integer.*
2. *Then* $k^2 + 2k + 1 = 3^2 + 2 \cdot 3 + 1 = 16$ *is a composite number.*
3. *Since* $16 = 4 \cdot 4$ *and* $1 < 4 < 16$, *by definition* $16$ *is a composite number.*
4. *Therefore* $k^2 + 2k + 1$ *is a composite number.*

# Example: find the flaw in proofs

## Example

*Find the flaw in the following proof of the same statement in previous example:*

1. *Let* $k = 3$ *be a positive integer.*
2. *Then* $k^2 + 2k + 1 = 3^2 + 2 \cdot 3 + 1 = 16$ *is a composite number.*
3. *Since* $16 = 4 \cdot 4$ *and* $1 < 4 < 16$*, by definition* $16$ *is a composite number.*
4. *Therefore* $k^2 + 2k + 1$ *is a composite number.*

## Solution

*Note that the statement is universal, so one (positive) example* $k = 3$ *is not enough to justify it.*

# Example: the correct proof

A correct proof of this statement is:

**Proof.**

Let $k$ be an arbitrary positive integer. Note that $k^2 + 2k + 1 = (k + 1) \cdot (k + 1)$. Since $k$ is positive, we have

$$k + 1 > 1.$$

And then

$$k^2 + 2k + 1 = (k + 1) \cdot (k + 1) > (k + 1) \cdot 1 = k + 1.$$

Since $k + 1$ is strictly between $1$ and $k^2 + 2k + 1$, by definition $k^2 + 2k + 1$ is a composite number. □

# HW #3 - this section

Section 4.1 Exercise 8, 13, 18, 28, 41, 58.