Topic for this Video: Section ~~4.1~~ 4.2: Dirct Proof and Counterexample II: Writing Advice

Remember that in Section 4.1 and in the video for Homework H04.1, you have seen discussion of proofs about only very basic concepts:

- *even* and *odd* numbers
- *composite* and *prime* numbers

And the proof structures that have used have also been very basic:

- Examples were used to prove true existential statements.
- Examples were used to disprove false universal statements.
- Univeral statements were proved by *Generalizing from the Generic Particular*.
- Universal conditional statements were proved using the *Method of Direct Proof*.

For reference, the definitions that we used are included on the next three pages.

Review of Mathematical Concepts

Definition of Even and Odd Numbers

Words: n *is even*

Meaning: $\exists k \in \boldsymbol{Z}(n = 2k)$

Words: n *is odd*

Meaning: $\exists k \in Z(n = 2k + 1)$

Definition of Composite Numbers

Words: n *is composite*

Meaning: $\exists r, s \in \boldsymbol{Z}\big((r > 1) \wedge (s > 1) \wedge (n = rs)\big)$

Definition of Prime Numbers

Words: n *is prime*

Meaning: $(n \in \boldsymbol{Z}) \wedge (n > 1) \wedge (n$ is not *composite*$)$

Review of Proof Methods that involve doing an example (or a bunch of examples)

Proving an Existential Statement

To prove the existential statement

$$\textit{There exists some } x \in D \textit{ such that } P(x).$$

one must produce an *example* of an $x \in D$ that makes $P(x)$ true.

Disproving a Universal Statement

To disprove the universal statement

$$\textit{For all } x \in D,\ P(x).$$

one must produce an *example* of an $x \in D$ that makes $P(x)$ false. Such an example is called a counterexample.

When a domain set D is a finite set, the *universal* statement

$$\forall x \in D\big(P(x)\big)$$

can be proven by confirming that $P(x)$ for each element of the domain. (This amounts to doing a bunch of examples.) This is called the ***Method of Exaustion***.

Review of Methods of General Proof

Generalizing from the Generic Particular

To show that *every* element of a set satisfies a certain property, suppose x is a *particular* but *arbitrarily chosen* element of the set, and show that x satisfies the property.

Method of Direct Proof

1. Express the statement to be proved in the form "For every $x \in D$, if $P(x)$ then $Q(x)$." (This step is often done mentally.)
2. Start the proof by supposing x is a particular but arbitrarily chosen element of D for which the hypothesis $P(x)$ is true. (This step is often abbreviated "Suppose $x \in D$ and $P(x)$.")
3. Show that the conclusion $Q(x)$ is true by using definitions, previously established results, and the rules for logical inference.

No new math concepts or proof methods are introduced in the reading of Section 4.2. The author just makes recommendations for writing good proofs and points out common mistakes. In this video, I will just do some examples of proofs of various sorts. In one of the examples, the concept of consecutive integers is used. Here is a definition

Definition of Consecutive Integers

Words: *two consecutive integers*

Meaning: numbers of the form $m, m+1$ where $m \in \boldsymbol{Z}$

Of course, this idea generalizes. Four consecutive integers would be numbers of the form $m, m+1, m+2, m+3$ where $m \in \boldsymbol{Z}$

And realize that the form can vary, too. For instance

- Two consecutive integers could be of the form $m-1, m$ where $m \in \boldsymbol{Z}$
- Four consecutive integers could be of the form $m-2, m-1, m, m+1$ where $m \in \boldsymbol{Z}$

.

[Example 1] Prove the following statement.

If m is any odd integer and n is any even integer, then $m^2 + n^2$ is odd.

Express formally

$\forall m, n \in \mathbb{Z}$ ($\overbrace{\text{If } m \text{ is odd and } n \text{ is even}}^{P}$ then $\overbrace{m^2+n^2 \text{ is odd}}^{Q}$)

Proof Structure (Direct proof)

(1) Suppose $m, n \in \mathbb{Z}$ and m is odd and n is even.

⋮ Some statements with justifications.

(*) therefore m^2+n^2 is odd

End of proof

Add more steps that are inevitable.

Proof

(1) Suppose $m,n \in \mathbb{Z}$ and m is odd and n is even.

(2) There exists an integer k such that $m=2k+1$ (by (1) and definition of odd)

(3) There exists an integer j such that $n=2j$ (by (1) and definition of even)

⋮ Some statements with justifications.

(**) there exists an integer h such that $m^2+n^2=2h+1$ (some justification)

(*) therefore m^2+n^2 is odd (by (**) and the definition of odd)

End of proof

Try to fill in the gap

Proof

(1) Suppose $m, n \in \mathbb{Z}$ and m is odd and n is even.

(2) There exists an integer k such that $m = 2k+1$ (by (1) and definition of odd)

(3) There exists an integer j such that $n = 2j$ (by (1) and definition of even)

(4) $m^2 + n^2 = (2k+1)^2 + 2j$ (by (2), (3))

$$= 4k^2 + 4k + 1 + 2j$$
$$= 4k^2 + 4k + 2j + 1$$
$$= 2(2k^2 + 2k + j) + 1$$

(5) Let $h = 2k^2 + 2k + j$. Observe that h is an integer

(6) there exists an integer h such that $m^2 + n^2 = 2h + 1$ (by 4, 5)

(7) therefore $m^2 + n^2$ is odd (by (6) and the definition of odd)

End of proof

[Example 2] Disprove the following statement.

Statement S *There exists an integer* $k \geq 4$ *such that* $2k^2 - 5k + 2$ *is prime*

Write S formally

Let Domain D be the set of integers ≥ 4.

S: $\exists k \in D\,(2k^2 - 5k + 2 \text{ is prime})$

$\sim S \equiv \sim(\exists k \in D\,(2k^2 - 5k + 2 \text{ is prime}))$

$\equiv \forall k \in D\,(\sim(2k^2 - 5k + 2 \text{ is prime}))$

$\equiv \forall k \in D\,(2k^2 - 5k + 2 \text{ is not prime})$

$\sim S$ is a universal statement.

To prove $\sim S$, we need a general proof

Proof Structure

(1) Suppose $k \in D$ (generic particular element)

$\vdots$ some steps here

(*) $2k^2 - 5k + 2$ is not prime (some justification)

End of proof

Proof Structure

this tells us k is an integer and $k \geq 4$

(1) Suppose $k \in D$ (generic particular element)

(2) $\underbrace{2k^2-5k+2} = \underbrace{\underbrace{(2k-1)}_{r}\underbrace{(k-2)}_{s}}$

Check $(2k-1)(k-2) =$
$= 2k^2-k-4k+2$
$= 2k^2-5k+2$ ✓

Let $r = 2k-1$
Since $k \geq 4$, we know $r \geq 7$

Let $s = k-2$
Since $k \geq 4$, we know $s \geq 2$

(3) So $2k^2-5k+2 = rs$ where $r \geq 7$ and $s \geq 2$

(4) So $2k^2-5k+2$ is composite (by (3) and the definition of composite)

(5) $2k^2-5k+2$ is not prime (by (4) and definition of prime)

End of proof

[Example 3] Prove or disprove following statement.

$n^3 - m^3$

For all integers m and n, if n − m is even, then $\cancel{n^3 - n^3}$ *is even.*

Solution Is this true or false? Not sure.

Experiment with some values of m, n

m	n	$n-m$	n^3-m^3
1	3	$3-1=2$ even	$3^3-1^3 = 27-1=26$ even.
1	5	$5-1=4$ even	$5^3-1^3 = 125-1 = 124$ even
2	4	$4-2=2$ even	$4^3-2^3 = 64-8=56$ even

Our statement seems to be true

It is a universal statement

So we cannot prove it by examples.

We must do a general proof.

Statement S For all integers m, n, If $n-m$ is even then n^3-m^3 is even

Proof Structure (Direct Proof)

(1) Suppose m, n are integers and $n-m$ is even

(*) Therefore n^3-m^3 is even

End of proof

Proof

(1) Suppose m, n are integers and $n-m$ is even

(2) There exists an integer k such that $n-m=2k$ (by 1 and definition of even)

(**) There exists an integer j such that $n^3-m^3=2j$

(*) Therefore n^3-m^3 is even (by (**) and definition of even)

End of proof

Proof

(1) Suppose m, n are integers and $n-m$ is even

(2) There exists an integer k such that $n-m=2k$ (by 1 and definition of even)

(3) $n^3-m^3 \underset{\uparrow \text{ factor}}{=} (n-m)\cdot(n^2+nm+m^2)$

Check $(n-m)(n^2+nm+m^2) =$

$= n^3+\cancel{n^2m}+\cancel{nm^2}-\cancel{mn^2}-\cancel{nm^2}-m^3$

$= n^3-m^3$

$= 2k\cdot(n^2+nm+m^2)$ by (2)

(4) Let $j = k\cdot(n^2+nm+m^2)$ observe that J is an integer

(5) There exists an integer j such that $n^3-m^3=2j$ (by 3, 4)

(6) Therefore n^3-m^3 is even (by (5) and definition of even)

End of proof

[Example 4] Prove or disprove following statement.

For every integer m, if m > 2, then $m^2 - 4$ *is composite.*

Not sure if this true or false. Try some values of m.

$m=3 \qquad 3^2-4 = 9-4 = 5$ which is prime, not composite

The statement is false. A counterexample is $m=3$.

Then 3 is an integer and $3>2$ and 3^2-4 is not composite.

[Example 5] Prove or disprove following statement.

The difference of the squares of any two consecutive integers is odd.

Recall: two consecutive integers can always be written

$m, m+1$ for some $m \in \mathbb{Z}$.

Rewrite the statement formally

$$\forall m \in \mathbb{Z}, \left(\underbrace{(m+1)^2 - m^2}_{} \text{ is } \underline{\text{odd}} \right)$$

This is the difference of the squares of two consecutive integers

Is this true or false?

<u>Experiment</u>

m	$m+1$	$(m+1)^2 - m^2$	
1	2	$4 - 1 = 3$	odd
2	3	$9 - 4 = 5$	odd
3	4	$16 - 9 = 7$	odd
-5	-4	$25 - 16 = 9$	odd
-1	0	$0 - 1 = -1$	odd

It seems that the statement is true. So we need a <u>general</u> proof.

$\forall m \in \mathbb{Z}, \left((m+1)^2 - m^2 \text{ is odd}\right)$

Proof Structure (Generalization from a generic particular element)

(1) Suppose $m \in \mathbb{Z}$ (generic particular element)

⋮ Some statements

(*) $(m+1)^2 - m^2$ is odd (Some justification)

End of proof

$\forall m \in \mathbb{Z}, \left((m+1)^2 - m^2 \text{ is odd} \right)$

Proof Structure (Generalization from a generic particular element)

(1) Suppose $m \in \mathbb{Z}$ (generic particular element)

$\vdots$ Some statements

(**) there exists an integer k such that $(m+1)^2 - m^2 = 2k+1$ (some justification)

(*) $(m+1)^2 - m^2$ is odd (by (**) and definition of odd)

End of proof

$\forall m \in \mathbb{Z}, \left((m+1)^2 - m^2 \text{ is odd}\right)$

Proof Structure (Generalization from a generic particular element)

(1) Suppose $m \in \mathbb{Z}$ (generic particular element)

(2) $(m+1)^2 - m^2 = \cancel{m^2} + 2m + 1 - \cancel{m^2}$ arithmetic

$= 2m + 1$

(3) let $k = m$ then k is an integer

(4) there exists an integer k such that $(m+1)^2 - m^2 = 2k+1$ (by (2) and (3))

(5) $(m+1)^2 - m^2$ is odd (by (4) and definition of odd)

End of proof