Topic for this Video: Section 4.4: Direct Proof and Counterexample IV: Divisibility

In this chapter, we have discussed the following kinds of proof structures:

- An *existential statement* that is *true* is proved by *giving an example*.
- A *universal statement* that is *false* is disproved by *giving an example* (a *counterexample*).
- A *univeral statement* with *finite domain* that is a *true* statement can be proved by *The Method of Exhaustion*, which amounts to doing a bunch of examples.
- A *univeral statement* with an *infinite domain* that is a *true* statement must be proved by the method of *Generalizing from the Generic Particular*. (NOT by an example!)
    - An *existential statement* with an *infinite domain* that is a *false* statement will have a negation that is a *universal statement*. To *disprove* the original existential statement, one must *prove* the negation that is a universal statement. This will require the method of *Generalizing from the Generic Particular*.
    - When the method of *Generalizing from the Generic Particular* is applied to the special case of proving a *universal conditional statement* with an *infinite domain*, the resulting proof structure is called the *Method of Direct Proof*.

We have studied and written proofs involving a growing list of defined mathematical terms:

- *even* and *odd numbers*
- *composite* and *prime numbers*
- *consecutive integers*
- *rational numbers* and *irrational numbers*
- the *zero product property*

In Section 4.4, we will learn no new proof structures, but we will add to our list of defined mathematical terms and mathematical concepts. The new mathematical term is *divisibility*. The new mathematical concept is *prime factorization*.

Definition of Divisibility

Symbol: $d|n$

Words: d *divides* n

Alternate words: d *is a divisor of* n

Alternate words: n *is divisible by* d

Meaning expressed in words, using division:

n and d are integers, and $\frac{n}{d}$ is an integer.

Meaning expressed in symbols, using *division*:

$$(n, d \in \boldsymbol{Z}) \wedge \left(\exists k \in \boldsymbol{Z}\left(\frac{n}{d} = k\right)\right)$$

Meaning expressed in symbols, using *multiplication*:

$$(n, d \in \boldsymbol{Z}) \wedge (d \neq 0) \wedge \big(\exists k \in \boldsymbol{Z}(n = dk)\big)$$

[Example 1] (a) Does $13|91$? Explain.

Spoken "Does 13 divide 91?"

yes because $\frac{91}{13} = 7$, which is an integer

Alternate explanation:

yes because $13 \neq 0$ and $91 = 13 \cdot 7$, and 7 is an integer.

(b) Does $91|13$? Explain.

Spoken: does 91 divide 13?

That is, is $\frac{13}{91}$ an integer?

No!

[Example 2] (a) Does 13|0? Explain.

Does 13 divide 0?

That is, is $\frac{0}{13}$ an integer?

Yes, because $\frac{0}{13} = 0$, which is an integer.

explaining using division

using multiplication: Yes, because $0 = 13 \cdot 0$, where 0 is an integer and $13 \neq 0$

(b) Does 0|13? Explain.

Does zero divide 13?

Answer: no

Two explanations

Explanation involving division: $\frac{13}{0}$ is not an integer.

Explanation involving multiplication: because d = 0

[Example 3] Suppose that n is an integer. Is $7n(25-15n^2)$ divisible by 35? Explain.

Answer: yes

Observe that

$$7n(25-15n^2) = 7n(5\cdot(5-3n^2))$$

$$= 7\cdot 5\cdot \underbrace{n\cdot(5-3n^2)}$$

$$= 35\cdot k$$

where $k = n\cdot(5-3n^2)$, which is an integer.

and $35 \neq 0$

[Example 4] Consider the statement

$$\text{If } ab|c \text{ then } a|c \text{ and } b|c.$$

(a) Rewrite the statement formally.

(b) Prove or disprove the statement.

(a) Solution

$\forall a,b,c \in \mathbb{Z}$ (If $ab|c$ then $a|c$ and $b|c$)

(b) The statement is true.

Observe: Universal Statement (universal conditional statement)

Domain $\mathbb{Z}$ is an infinite set.

So we need to prove using the structure called Direct Proof.

$\forall a,b,c \in \mathbb{Z}$ (If $ab|c$ then $a|c$ and $b|c$)

Proof (Direct proof)

(1) Suppose $a,b,c \in \mathbb{Z}$ and that $ab|c$ (generic particular elements)

(2) So $ab \neq 0$ and there exists an integer k such that $c = ab \cdot k$ (by (1)) and definition of divides)

(3) So $a \neq 0$ and $b \neq 0$ (by (2) and the zero product property.)

(4) Let $n = a \cdot k$. Then observe that n is an integer and $c = bn$

(5) Let $m = b \cdot k$. Then observe that m is an integer and $c = am$.

((6) $b \neq 0$ and there exists an integer n such that $c = bn$ (by (3),(4))

((7) $a \neq 0$ and there exists an integer m such that $c = a \cdot m$ (by (3),(5))

(8) Therefore $a|c$ and $b|c$ ((6) and (7) and definition of divides)

End of proof.

[Example 5] Consider the statement

$$\text{If } a|bc \text{ then } a|b \text{ and } \cancel{b|c}.\quad a|c,$$

(a) Rewrite the statement formally.

(b) Prove or disprove the statement.

(a) S: $\forall a,b,c \in \mathbb{Z}$ (If $a|bc$ then $a|b$ and $a|c$)

(b) Statement S is false. To disprove it, we must provide a counterexample. That is, we need an example of a,b,c that make $\sim S$ true.

The negation of S is this statement.

$$\sim S \equiv \exists a,b,c \in \mathbb{Z} \left(a|bc \text{ AND } \left(a\nmid b \text{ or } a \nmid c \right)\right)$$

our example (our counterexample)

Let $a,b,c = 6,4,3$

we found the integer 2 that works.

explanation of why the counterexample works

observe that $6|4\cdot 3$ because $4\cdot 3 = 6\cdot 2$

$a|b\cdot c$

but $6|4$ is false. $\frac{4}{6}$ is not an integer. $6\nmid 4$ $a\nmid b$.

and $6|3$ is false $\frac{3}{6}$ is not an integer. $6\nmid 3$ $a\nmid c$

Examples involving both the *new* term *divisibility* and *previously defined terms*.

Example involving *divisibility* and *even numbers*

[Example 6] Consider the statement

The product of any two even integers is a multiple of 4.

(a) Rewrite the statement formally.

(b) Prove or disprove the statement.

$\forall$ even integers m, n (mn is a multiple of 4)

$\forall$ even integers m, n ($\exists$ integer k such that $mn = 4k$)

Proof

(1) Suppose m, n are even integers (generic particular elements)

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

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

(4) Then $m \cdot n = (2j) \cdot (2p)$ (by, 3, 4)

$= 4 \cdot (jp)$

(5) let $k = jp$. Observe that k is an integer and $mn = 4k$

(6) There exists an integer k such that $mn = 4k$ (by (5))

End of Proof

Examples involving *divisibility* and *consecutive integers*

[Example 7] Consider the statement

The sum of any three consecutive integers is a multiple of 3.

(a) Rewrite the statement formally.

(b) Prove or disprove the statement.

Solution

three consecutive integers can always be written $m, m+1, m+2$.

$\forall m \in \mathbb{Z}\ (m + (m+1) + (m+2)$ is a multiple of $3)$

Proof

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

(2) Then $m+(m+1)+(m+2) = 3m+3$ by arithmetic
$= 3(m+1)$ factored

(3) Let $k = m+1$ then k is an integer (because m is integer)

(4) There exists some integer k such that $m+(m+1)+(m+2) = 3k$ (by 2,3)

(5) $m+(m+1)+(m+2)$ is a multiple of 3.
(by (4) and definition of is a multiple of)

End of Proof

The Unique Factorization Theorem

Theorem 4.4.5 Unique Factorization of Integers

Given any integer $n > 1$, there exist

- a positive integer k
- distinct prime numbers $p_1 < p_2 < \cdots < p_k$
- positive integers $e_1, e_2, \ldots, e_k$

such that n can be written as the product

$$n = p_1^{e_1} p_2^{e_2} \ldots p_k^{e_k}$$

This expression is called the ***standard ~~factord~~ form*** of n.

factored

[Example 8] Let $n = 428064$

(a) Find the unique factorization of n.

(b) Write the prime factorization for n^3.

(c) What is the least positive integer m so that nm is a perfect cube.

(d) Write the product nm as a perfect cube.

Solution

$k=4$

$p_1=2,\ p_2=3,\ p_3=7,\ p_4=13$

$e_1=5,\ e_2=1,\ e_3=3,\ e_4=1$

(a) $n = 428064 = 2^5 \cdot 3 \cdot 7^3 \cdot 13$

(b) $n^3 = (2^5 \cdot 3 \cdot 7^3 \cdot 13)^3 = 2^{15} \cdot 3^3 \cdot 7^9 \cdot 13^3$

(c) We need nm to be a perfect cube.

So the prime factorization of nm needs all exponents to be multiples of 3.

$n \cdot m = (2^5 \cdot 3 \cdot 7^3 \cdot 13) \cdot m$

this needs to include $2^1 \cdot 3^2 \cdot 13^2$

Let $m = 2^1 \cdot 3^2 \cdot 13^2 = 3042$

Then $n \cdot m = (2^5 \cdot 3 \cdot 7^3 \cdot 13) \cdot (2^1 \cdot 3^2 \cdot 13^2) = 2^6 \cdot 3^3 \cdot 7^3 \cdot 13^3$

(d) $nm = 2^6 \cdot 3^3 \cdot 7^3 \cdot 13^3 = 1{,}302{,}170{,}688 = (2^2 \cdot 3 \cdot 7 \cdot 13)^3 = (1092)^3$

[Example 9] Let $n = 17!$

(a) Write n in standard factored form.

(b) Withough computing the value of n^3, determine how many zeros are at the end of n^3 when it is written in decimal form. Explain.

Solution

(a) $n = 17! = 17 \cdot 16 \cdot 15 \cdot 14 \cdot 13 \cdot 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 \cdot 7 \cdot 6 \cdot 5 \cdot 4 \cdot 3 \cdot 2 \cdot 1$

$= 17 \cdot 2^4 \cdot (3^1 \cdot 5^1) \cdot (2^1 \cdot 7) \cdot 13 \cdot (2^2 \cdot 3^1) \cdot 11 \cdot (2^1 \cdot 5^1) \cdot 3^3 \cdot 2^3 \cdot 7 \cdot (2^1 \cdot 3^1) \cdot 5^1 \cdot 2^2 \cdot 3^1 \cdot 2^1$

$= 2^{15} \cdot 3^7 \cdot 5^3 \cdot 7^2 \cdot 11^1 \cdot 13^1 \cdot 17$

(b) Standard factored form of n^3 is

$n^3 = (2^{15} \cdot 3^7 \cdot 5^3 \cdot 7^2 \cdot 11^1 \cdot 13^1 \cdot 17^1)^3 = 2^{45} \cdot 3^{21} \cdot 5^9 \cdot 7^6 \cdot 11^3 \cdot 13^3 \cdot 17^3$

Each zero at the end of the decimal form of n^3 will come from $(2 \cdot 5)$ in the prime factorization of n^3.

Observe $n^3 = 2^{45} \cdot 5^9 \cdot$ a bunch of factors that don't involve 2 or 5.

$= \underbrace{2^9 \cdot 5^9} \cdot \underbrace{2^{36} \cdot \text{a bunch of factors that don't include 2 or 5.}}$

$= \underbrace{(10)^9} \cdot$ red integer that does not have 5 as a factor.

So there will be 9 zeros at the end of n^3