Topic for this Video:

Section 4.5: Direct Proof and Counterexample V:

Division into Cases and the Quotient-Remainder Theorem

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*
- the concept of *divisibility*

In Section 4.5, we will add to our list of defined mathematical terms and mathematical concepts. The new mathematical concepts are the absolute value function and also concepts related to the *Quotient Remainder Theorem*. We will also learn about a new kind of proof structure: *Division into Cases*. (used within the existing proof structure of Direct Proof)

We will start by discussing the *Quotient Remainder Theorem*.

Consider this collection of equations

$$\begin{gathered}\vdots\\ 71 = 9 \cdot 10 + (-19)\\ 71 = 9 \cdot 9 + (-10)\\ 71 = 9 \cdot 8 + (-1)\\ 71 = 9 \cdot 7 + 8\\ 71 = 9 \cdot 6 + 17\\ 71 = 9 \cdot 5 + 26\\ \vdots\end{gathered}$$

There is an infinite set of true equations involving 71 and 9, but only one equation

$$71 = 9 \cdot 7 + 8$$

has a red number that satisfies the inequality

$$0 \le 8 < 9$$

.

Now consider this collection of equations

$$\vdots$$

$$72 = 9 \cdot 10 + (-18)$$

$$72 = 9 \cdot 9 + (-9)$$

$$72 = 9 \cdot 8 + 0$$

$$72 = 9 \cdot 7 + 9$$

$$72 = 9 \cdot 6 + 18$$

$$72 = 9 \cdot 5 + 27$$

$$\vdots$$

There is an infinite set of true equations involving 72 and 9, but only one equation

$$72 = 9 \cdot 6 + 0$$

has a red number that satisfies the inequality

$$0 \le 0 < 9$$

.

Finally, consider this collection of equations

$$\vdots$$

$$-71 = 9 \cdot (-10) + 19$$

$$-71 = 9 \cdot (-9) + 10$$

$$-71 = 9 \cdot (-8) + 1$$

$$-71 = 9 \cdot (-7) + (-8)$$

$$-71 = 9 \cdot (-6) + (-17)$$

$$-71 = 9 \cdot (-5) + (-26)$$

$$\vdots$$

There is an infinite set of true equations involving -71 and 9, but only one equation

$$-71 = 9 \cdot (-8) + 1$$

has a red number that satisfies the inequality

$$0 \leq 1 < 9$$

.

Those three examples should convince you of the truth of the following important theorem.

Theorem 4.1.1 The Quotient-Remainder Theorem (*QRT*)

Informal presentation:

Given any integer n and any positive integer d,

there exist unique integers q and r such that $n = dq + r$ and $0 \le r < d$

Formal (symbolic)presentation:

$$\forall n \in \boldsymbol{Z}, d \in \boldsymbol{Z}^+ \left(\exists! q, r \in \boldsymbol{Z}\big((n = dq + r) \wedge (0 \le r < d)\big)\right)$$

Additional terminology

The number d is called the ***divisor***.

The number q is called the ***quotient***. Note that q can be any integer (including 0).

The number r is called the ***remainder***. Note that r must be a non-negative integer.

Mark's special terminology

Words: The integer equation $n = dq + r$ is in ***special QRT form***

Meaning: the integers r, d satisfy the requirement $0 \le r < d$

.

There is a related definition of two expressions involving the words div and mod

Definition of $\boldsymbol{div}$ and $\boldsymbol{mod}$.

Symbol: $n\ div\ d$

Usage: n is an integer and d, is a positive integer.

Meaning: the unique integer q such that $n = dq + r$ and $0 \leq r < d$

Symbol: $n\ mod\ d$

Usage: n is an integer and d, is a positive integer.

Meaning: the unique integer r such that $n = dq + r$ and $0 \leq r < d$

[Example 1] (Similar to 4.5#8)

(a) Find 28 *div* 5 and 28 *mod* 5

(b) Find −28 *div* 5 and −28 *mod* 5

(c) Find 30 *div* 5 and 30 *mod* 5

(d) Find 3 div 5 and 3 mod 5

Solution

(a) Find 28 div 5 and 28 mod 5.

$\underbrace{28 \text{ div } 5}_{\text{the special } q}$ $\underbrace{28 \text{ mod } 5}_{\text{the special } r}$

Strategy
- Write the special equation

$$n = dq + r \quad \text{satisfying} \quad 0 \le r < d$$

- Then identify 28 div 5 = q and 28 mod 5 = r

$$\underset{n}{28} = \underset{d}{5} \cdot \underset{q}{5} + \underset{r}{3}$$

28 div 5 = 5

28 mod 5 = 3

(b) Find -28 div 5 and -28 mod 5

Solution Start by writing the special equation $n = dq + r$

$$\underbrace{-28}_{} = 5 \cdot \underset{q}{(-6)} + \underset{r}{2} \qquad 0 \le 2 < 5$$

$$0 \le r < d$$

-28 div $5 = -6$ $\qquad$ -28 mod $5 = 2$

(c) Find 30 div 5 and 30 mod 5

Solution Write special equation

$$30 = 5 \cdot \underset{q}{(6)} + \underset{r}{0}$$

30 div $5 = 6$ $\qquad$ 30 mod $5 = 0$

(d) find 3 div 5 and 3 mod 5

Solution: write special equation $3 = 5 \cdot \underset{q}{(0)} + \underset{r}{3}$

3 div $5 = 0$

3 mod $5 = 3$

[Example 2] (similar to 4.5#21)

If c is an integer such that $c \; mod \; 13 = 5$, then what is $6c \; mod \; 13$?

Strategy

$c \bmod 13 = 5$

$\Downarrow$

Special equation involving $c, 13, 5$

$\Downarrow$

Special equation involving $6c, 13$

$\Downarrow$

identify the value of r

$c \bmod 13 = 5$

$$\underset{n}{c} = \underset{d}{13}q + 5$$

multiply this equation by 6

$$6c = 6(13q + 5) = 13 \cdot 6q + 30$$

$$= 13 \cdot 6q + 26 + 4$$

$$\underset{n}{6c} = \underset{d}{13} \cdot \underbrace{(6q + 2)} + \underset{r}{4} \qquad 0 \le 4 < 13$$

$6c \bmod 13 = 4$

Using the Quotient-Remainder Theorem in proofs

[Example 3] Suppose that n is an integer.

(a) What does the Quotient Remainder Theorem with $d = 2$ tell us about n?

There exist unique integers q, r such that $n = 2q + r$ and $\underbrace{0 \leq r < 2}$

There are only two possibilities!

That is

There exists integer q such that $n = 2q$

or there exists an integer q such that $n = 2q + 1$

(b) What does the Quotient Remainder Theorem with $d = 3$ tell us about n?

There exist unique integers q, r such that $n = 3q + r$ and $0 \le r < 3$

Rewrite with actual values for r

$$\big(\exists q \in \mathbb{Z}\,(n = 3q)\big) \text{ or } \big(\exists q \in \mathbb{Z}\,(n = 3q+1)\big) \text{ or } \big(\exists q \in \mathbb{Z}\,(n = 3q+2)\big)$$

Proof by Division into Cases

Recall the *Rules of Inference* (which are just known *Valid Argument Forms*).

TABLE 2.3.1 Valid Argument Forms

Modus Ponens	$p \rightarrow q$ p $\therefore q$	**Elimination**	**a.** $p \vee q$ $\sim q$ $\therefore p$ **b.** $p \vee q$ $\sim p$ $\therefore q$
Modus Tollens	$p \rightarrow q$ $\sim q$ $\therefore \sim p$	**Transitivity**	$p \rightarrow q$ $q \rightarrow r$ $\therefore p \rightarrow r$
Generalization	**a.** p $\therefore p \vee q$ **b.** q $\therefore p \vee q$	**Proof by Division into Cases**	$p \vee q$ $p \rightarrow r$ $q \rightarrow r$ $\therefore r$
Specialization	**a.** $p \wedge q$ $\therefore p$ **b.** $p \wedge q$ $\therefore q$		
Conjunction	p q $\therefore p \wedge q$	**Contradiction Rule**	$\sim p \rightarrow \mathbf{c}$ $\therefore p$

The *Quotient Remainder Theorem* (*QRT*) can be used to build proofs that use the method of *Division into Cases*.

$$\boxed{\begin{array}{l} p \vee q \\ p \rightarrow r \\ q \rightarrow r \\ \therefore r \end{array}}$$

[Example 4] (similar to 4.5#27) Use the Quotient-Remainder Theorem with divisor $d = 3$ to prove that the square of any integer has the form $3k$ or $3k + 1$ for some integer k.

$$\forall n \in \mathbb{Z}\left(\left(\exists k \in \mathbb{Z}\,(n^2 = 3k)\right) \text{ or } \left(\exists k \in \mathbb{Z}\,(n^2 = 3k+1)\right)\right)$$

Proof

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

(2) $(\exists q \in \mathbb{Z}\,(n = 3q))$ or $(\exists q \in \mathbb{Z}\,(n = 3q+1))$ or $(\exists q \in \mathbb{Z}\,(n = 3q+2))$ by QRT with $d = 3$

(3) (Case 1) Suppose $n = 3q$ for some integer q

(4) Then $n^2 = (3q)^2 = 3 \cdot 3q^2$

(5) let $k = 3q^2$. Observe that k is an integer and $n^2 = 3k$

So the conclusion is true in this case.

(6) (case 2) Suppose $n = 3q+1$ for some integer q

(7) Then $n^2 = (3q+1)^2 = 9q^2 + 6q + 1 = 3(3q^2 + 2q) + 1$

(8) Let $k = 3q^2 + 2q$. Observe that k is an integer and $n^2 = 3k+1$

So the conclusion is true in this case.

(9) (Case 3) Suppose $n = 3q + 2$

(10) Then $n^2 = (3q+2)^2 = 9q^2 + 12q + 4 =$

$$= 9q^2 + 12q + 3 + 1$$

$$= 3(3q^2 + 3q + 1) + 1$$

(11) Let $k = 3q^2 + 3q + 1$. Observe that k is an integer and $n^2 = 3k+1$

So our conclusion is true in this case, as well.

(12) Observe that the conclusion is true in every case

Therefore, $(\exists k \in \mathbb{Z}(n^2 = 3k))$ or $(\exists k \in \mathbb{Z}(n^2 = 3k+1))$

End of proof.

The Absolute Value Function

You are familiar with the behavior of the absolute value function when the thing inside is a *number*. For example,

$$|5| = 5$$

$$|-5| = 5$$

$$|0| = 0$$

But you are probably not so familiar with the absolute value in abstract settings, where the thing inside the absolute value involves a *variable*. The absolute value is defined piecewise. That is, the meaning of the symbol $|x|$ depends on which piece of the domain x is in.

Definition of the Absolute Value

Symbol: $|x|$

Spoken: the ***absolute value of x***

Usage: x is a real number

Meaning: $|x|$ is a real number, defined by

$$|x| = \begin{cases} x & \text{if } x \geq 0 \\ -x & \text{if } x < 0 \end{cases}$$

Less Appreviated Expression:

$$|x| = \begin{cases} x & \text{if } x > 0 \\ 0 & \text{if } x = 0 \\ -x & \text{if } x < 0 \end{cases}$$

Example: $|-5| = -(-5) = 5$

observe that $-5 < 0$

So use formula $|x| = -x$

[Example 5] Prove that for every real number r, $|-r| = |r|$

Proof

(1) Let r be a real number (generic particular element)

(2) Then $(r > 0)$ or $(r = 0)$ or $(r < 0)$ Property of real numbers

(3) Case 1 Suppose $r > 0$

(4) Then $-r < 0$

(5) So $|-r| = -(-r) = r$

use appropriate formula

and $|r| = r$

use appropriate formula

(6) So in this case, $|-r| = |r|$

(7) (Case 2) Suppose $r = 0$

(8) then $|r| = |0| = 0$

by definition of absolute value.

then $|-r| = |-0| = |0| = 0$

definition of abs value

(9) So $|-r| = |r|$ in this case as well

(10) (Case 3) Suppose $r < 0$

(11) Then $-r > 0$

(12) So $|-r| = -r$

use appropriate form

(13) and $|r| = -r$

use appropriate form

(14) Observe that $|-r| = |r|$ in this case as well

(15) We have shown that $|-r| = |r|$ (because it is true in every case)

End

[Example 6] Prove that all real numbers x, y, $|x| \cdot |y| = |xy|$

Proof

(1) Let x, y be real numbers (generic particular elements)

(2) Then $((x>0) \wedge (y>0))$ or $((x>0) \wedge (y=0))$ or $((x>0) \wedge (y<0))$
or $((x=0) \wedge (y>0))$ or $((x=0) \wedge (y=0))$ or $((x=0) \wedge (y<0))$
or $((x<0) \wedge (y>0))$ or $((x<0) \wedge (y=0))$ or $((x<0) \wedge (y<0))$

Case 1 both $x>0$ and $y>0$

Case 2 both $x<0$ and $y<0$

Case 3 one is >0 and one is <0

Case 4 one or both is equal to zero.