Math 417 – Second Day – In class

Bruce Reznick
University of Illinois at Urbana-Champaign

August 26, 2020

I'd like to highlight a few things from the lecture I distributed Tuesday evening, and based on your emails. I got some questions about THEOREM 3

I'd like to highlight a few things from the lecture I distributed Tuesday evening, and based on your emails. I got some questions about THEOREM 3

THEOREM 3: If $n \in \mathbb{Z}$ and $d \in \mathbb{N}$, then there is a unique integer $r \in \{0, 1, \ldots, d-1\}$ so that $n \equiv r \mod d$.

I'd like to highlight a few things from the lecture I distributed Tuesday evening, and based on your emails. I got some questions about THEOREM 3

THEOREM 3: If $n \in \mathbb{Z}$ and $d \in \mathbb{N}$, then there is a unique integer $r \in \{0, 1, \ldots, d-1\}$ so that $n \equiv r \mod d$.

PROOF: Use the division algorithm; divide n by d with remainder r. To be precise, let $t = \lfloor \frac{n}{d} \rfloor$, the largest integer $\leq \frac{n}{d}$. Then

$$t \leq \frac{n}{d} < t+1 \implies dt \leq n < dt + d \implies 0 \leq n - dt < d$$

so $n - dt = r$ for some $r \in \{0, 1, \ldots, d-1\}$, and so $n \equiv r \mod d$.

I'd like to highlight a few things from the lecture I distributed Tuesday evening, and based on your emails. I got some questions about THEOREM 3

THEOREM 3: If $n \in \mathbb{Z}$ and $d \in \mathbb{N}$, then there is a unique integer $r \in \{0, 1, \ldots, d-1\}$ so that $n \equiv r \mod d$.

PROOF: Use the division algorithm; divide n by d with remainder r. To be precise, let $t = \lfloor \frac{n}{d} \rfloor$, the largest integer $\leq \frac{n}{d}$. Then

$$t \leq \frac{n}{d} < t+1 \implies dt \leq n < dt + d \implies 0 \leq n - dt < d$$

so $n - dt = r$ for some $r \in \{0, 1, \ldots, d-1\}$, and so $n \equiv r \mod d$.

On the next page, I will give an illustration of the proof when $n = 12$ and $d = 5$.

We have $\frac{12}{5} = 2.4$, and the largest integer ≤ 2.4 is 2. So the first part of the last equation is

$$2 \leq 2.4 < 3$$

We have $\frac{12}{5} = 2.4$, and the largest integer ≤ 2.4 is 2. So the first part of the last equation is

$$2 \leq 2.4 < 3$$

We got 2.4 from dividing by 5, so now I'll multiply through by 5

$$2 \cdot 5 \leq 12 < 3 \cdot 5$$

We have $\frac{12}{5} = 2.4$, and the largest integer ≤ 2.4 is 2. So the first part of the last equation is

$$2 \leq 2.4 < 3$$

We got 2.4 from dividing by 5, so now I'll multiply through by 5

$$2 \cdot 5 \leq 12 < 3 \cdot 5$$

Now I'll subtract $2 \cdot 5$ from this equation

$$0 \leq 12 - 2 \cdot 5 < 5$$

We have $\frac{12}{5} = 2.4$, and the largest integer ≤ 2.4 is 2. So the first part of the last equation is

$$2 \leq 2.4 < 3$$

We got 2.4 from dividing by 5, so now I'll multiply through by 5

$$2 \cdot 5 \leq 12 < 3 \cdot 5$$

Now I'll subtract $2 \cdot 5$ from this equation

$$0 \leq 12 - 2 \cdot 5 < 5$$

In general, we have $d(t+1) - dt = d$ and an integer r which satisfies $0 \leq r < d$ must be one of $\{0, 1, \ldots, d-1\}$.
Here, $r = 12 - 2 \cdot 5 = 12 - 10 = 2 \in \{0, 1, 2, 3, 4\}$, and what we really want is that

$$12 \equiv 2 \mod 5.$$

People wanted to see the uniqueness proof again, so I will do it bit more slowly; at heart, it's a proof by contradiction.

People wanted to see the uniqueness proof again, so I will do it bit more slowly; at heart, it's a proof by contradiction.

Why is r unique? Suppose we had two different representations:

$$n = dt_1 + r_1, \qquad r_1 \in \{0, 1, \ldots, d-1\}$$
$$n = dt_2 + r_2, \qquad r_2 \in \{0, 1, \ldots, d-1\}$$

People wanted to see the uniqueness proof again, so I will do it bit more slowly; at heart, it's a proof by contradiction.

Why is r unique? Suppose we had two different representations:

$$n = dt_1 + r_1, \qquad r_1 \in \{0, 1, \ldots, d-1\}$$
$$n = dt_2 + r_2, \qquad r_2 \in \{0, 1, \ldots, d-1\}$$

Subtract these two equations to get

$$n - n = 0 = d(t_1 - t_2) + (r_1 - r_2) \implies r_1 - r_2 = -d(t_1 - t_2) = d(t_2 - t_1).$$

People wanted to see the uniqueness proof again, so I will do it bit more slowly; at heart, it's a proof by contradiction.

Why is r unique? Suppose we had two different representations:

$$n = dt_1 + r_1, \qquad r_1 \in \{0, 1, \ldots, d-1\}$$
$$n = dt_2 + r_2, \qquad r_2 \in \{0, 1, \ldots, d-1\}$$

Subtract these two equations to get

$$n-n = 0 = d(t_1-t_2)+(r_1-r_2) \implies r_1-r_2 = -d(t_1-t_2) = d(t_2-t_1).$$

This means that $r_1 - r_2$ is a multiple of d. But $0 \leq r_1, r_2 \leq d-1$. The largest $r_1 - r_2$ can be is $(d-1) - 0 = d-1$ and the smallest $r_1 - r_2$ can be is $0 - (d-1) = -(d-1)$:

$$r_1 - r_2 \in [-(d-1), (d-1)].$$

People wanted to see the uniqueness proof again, so I will do it bit more slowly; at heart, it's a proof by contradiction.

Why is r unique? Suppose we had two different representations:

$$n = dt_1 + r_1, \qquad r_1 \in \{0, 1, \ldots, d-1\}$$
$$n = dt_2 + r_2, \qquad r_2 \in \{0, 1, \ldots, d-1\}$$

Subtract these two equations to get

$$n-n = 0 = d(t_1-t_2)+(r_1-r_2) \implies r_1-r_2 = -d(t_1-t_2) = d(t_2-t_1).$$

This means that $r_1 - r_2$ is a multiple of d. But $0 \leq r_1, r_2 \leq d-1$. The largest $r_1 - r_2$ can be is $(d-1) - 0 = d-1$ and the smallest $r_1 - r_2$ can be is $0 - (d-1) = -(d-1)$:

$$r_1 - r_2 \in [-(d-1), (d-1)].$$

The multiples of d are $\{\ldots, -2d, -d, 0, d, 2d, \ldots\}$ and so the only multiple of d in $[-(d-1), (d-1)]$ is 0, so $r_1 - r_2 = 0$ and $r_1 = r_2$ and $t_1 = t_2$, and the two representations are the same.

Now something different. In the lecture part, We've seen that the only group with two elements is the cyclic one. What about three?

Now something different. In the lecture part, We've seen that the only group with two elements is the cyclic one. What about three?

Suppose $G = \{e, x, y\}$, three different elements, where e is the identity. What we already know about the multiplication table:

Now something different. In the lecture part, We've seen that the only group with two elements is the cyclic one. What about three?

Suppose $G = \{e, x, y\}$, three different elements, where e is the identity. What we already know about the multiplication table:

$*$	e	x	y
e	e	x	y
x	x	?	?
y	y	?	?

Now something different. In the lecture part, We've seen that the only group with two elements is the cyclic one. What about three?

Suppose $G = \{e, x, y\}$, three different elements, where e is the identity. What we already know about the multiplication table:

$*$	e	x	y
e	e	x	y
x	x	?	?
y	y	?	?

What can $x * x$ be? It has to be one of $\{e, x, y\}$ and, since $e * x = x$, if $x * x = x$, then $e = x$, which is impossible, so $x * x \neq x$. Thus, either $x * x = e$ or $x * x = y$. We'll explore these cases now.

Suppose $x * x = e$. Then the table becomes

$*$	e	x	y
e	e	x	y
x	x	e	?
y	y	?	?

Suppose $x * x = e$. Then the table becomes

$*$	e	x	y
e	e	x	y
x	x	e	?
y	y	?	?

What about $x * y$?

Suppose $x * x = e$. Then the table becomes

$*$	e	x	y
e	e	x	y
x	x	e	?
y	y	?	?

What about $x * y$?

It has to be different from $x * e = x$ and $x * x = e$, because remember that the rows have to be a permutation of $G = \{e, x, y\}$. This means that $x * y = y$. But $e * y = y$, and that shows that this is impossible. (Columns have to be permutations too.)

Suppose $x * x = e$. Then the table becomes

$*$	e	x	y
e	e	x	y
x	x	e	?
y	y	?	?

What about $x * y$?

It has to be different from $x * e = x$ and $x * x = e$, because remember that the rows have to be a permutation of $G = \{e, x, y\}$. This means that $x * y = y$. But $e * y = y$, and that shows that this is impossible. (Columns have to be permutations too.)

In other words, this multiplication table cannot be completed and no such group exists!

Since $x * x = e$ is impossible, we are forced to conclude that $x * x = y$

$*$	e	x	y
e	e	x	y
x	x	y	?
y	y	?	?

And now, to complete the row, we have to have $x * y = e$, and by looking at the columns, we can complete the last row:

$*$	e	x	y
e	e	x	y
x	x	y	e
y	y	e	x

Since $x * x = e$ is impossible, we are forced to conclude that $x * x = y$

$*$	e	x	y
e	e	x	y
x	x	y	?
y	y	?	?

And now, to complete the row, we have to have $x * y = e$, and by looking at the columns, we can complete the last row:

$*$	e	x	y
e	e	x	y
x	x	y	e
y	y	e	x

This table actually has a nice interpretation. I'll write it again, but with $y = x * x = x^2$:

$*$	e	x	x^2
e	e	x	x^2
x	x	x^2	e
x^2	x^2	e	x

This table actually has a nice interpretation. I'll write it again, but with $y = x * x = x^2$:

$*$	e	x	x^2
e	e	x	x^2
x	x	x^2	e
x^2	x^2	e	x

This is basically the same thing as $(\mathbb{Z}/3\mathbb{Z}, \oplus)$. I'll just write "0" for "$[0]_3$", etc

$\oplus$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1