Discrete Math

Lecture 17

Proofs

What is a proof?

an explanation of a math. fact

100% convincing

100% clear

step-by-step

each step is carefully explained

Theorem

Propositions

↳ "small theorems"

examples

The Fundamental Theorem of Algebra

Every degree-n polynomial has at most n roots.

FTC

If a function $f : [a, b] \to \mathbb{R}$ is continuous, then

$$\int_a^b f(x)\,dx = F(b) - F(a), \text{ where } F'(x) = f(x).$$

---

① most theorems & propositions are

$P \Rightarrow Q$ (or $P \Leftrightarrow Q$)

② proofs use definitions & previous facts

ex $0 + x = x$

Definitions of certain sets ($\emptyset, \mathbb{N}, \mathbb{Z}, \ldots$) will be used

also some familiar concepts about $\mathbb{N}, \mathbb{Z}$

Definition 3.1. (Divides & Divisors). *An integer $a \in \mathbb{Z}$ is said to* ***divide*** *another integer, $b \in \mathbb{Z}$, if $\exists q \in \mathbb{Z}$ such that*

$$b = q \cdot a.$$

*This is notated by writing $a|b$, where the line "$|$" is pronounced "**divides.**" For instance, you are already aware that 5 divides 10, but now we can write $5|10$; this is a true statement because*

$$10 = 2 \cdot 5.$$

*We also use the word **divisor** in this situation. That is, the phrase "a **divides** b" can be restated as "a **is a divisor of** b." This allows us to write and speak sentences like "5 is a **divisor of** 10." Indeed, one can write down* all *of the divisors of 10 (or any integer):*

$$\textit{the set of the divisors of 10} = \{-10, -5, -2, -1, 1, 2, 5, 10\}.$$

*Make certain you can use the definitions of "**divides**" and "**divisors**" to understand why each number in the set above belongs there. A good way to check that you're understanding these is to answer a questions like these:* what are all the divisors of 9? What about the divisors of 5? 100? 24?

*Note: These definitions only apply to integers, even though you know how to divide other types of numbers (like rationals and reals). Also, some us the synonym "**factor**" for "**divisor.**"*

ex) $3|8$ is false

$8 = q \cdot 3 = 3 \cdot q, \quad q \in \mathbb{Z}$

no $q \in \mathbb{Z}$ will solve $3q = 8$

$q=1$ fails
$q=2$
$q=3$

$\boxed{3 \nmid 8}$ ← 3 is not a divisor of 8.

you're understanding these is to answer a questions like these: what are all the divisors of 9? What about the divisors of 5? 100? 24?

			why ?
1 is a divisor	$1 \mid 9$	9 is a mult. of 1	$9 = 9 \cdot 1$ ✓
-1 is a divisor	$(-1) \mid 9$	9 is a mult. of -1	$9 = (-9) \cdot (-1)$ ✓
3 is a divisor	$3 \mid 9$	9 is a mult. of 3	$9 = 3 \cdot 3$
-3 is a divisor	$(-3) \mid 9$	⋮	$9 = (-3) \cdot (-3)$
9 is a divisor	$9 \mid 9$		$9 = 1 \cdot 9$
-9 is a divisor	$(-9) \mid 9$		$9 = (-1) \cdot (-9)$

divisors of 5: $\{1, 5, -1, -5\}$

divisors of 100: $\{-100, -50, -25, -20, -10, -5, -1, \ldots, 50, 100\}$

divisors of 24: $\{-24, -12, -8, -6, -4, -3, -2, 2, 3, 4, 6, 8, 12, 24\}$

note: lots of times we focus on positive divisors

Definition 3.2. (Multiple). *An integer $b \in \mathbb{Z}$ is said to be* ***a multiple of*** *another integer $a \in \mathbb{Z}$ if $\exists q \in \mathbb{Z}$ such that*

$$b = q \cdot a.$$

In other words, the phrase "b ***is a multiple of*** *a" is another way of saying "a|b." (Also 'b* ***is a multiple of*** *a" means "a is a divisor of b.") For instance, we can say "10 is a multiple of 5."*

$$\underbrace{b = q \cdot a}_{a|b}$$

"b is a <u>multiple</u> of a"

ex| $6|42$ "six divides foray-two"

$42 = q \cdot 6$

$q = 7$

"42 is a <u>multiple</u> of 6"

ex| 9 is a multiple of 3 ✓

$(3|9 \quad 9 = q \cdot 3)$

Definition 3.3. (Prime). *A natural number $p \in \mathbb{N}$ is a **prime number** if it has exactly two (positive) divisors. For instance, 7 is prime because the only natural numbers that divide it are* 1 *and* 7. 10 *is **not prime** because it has more than two (positive) divisors, and* 1 *is **not prime** because it only has one, single (positive) divisor.*

Compare this definition with the more common one that sounds something like this: "a number p is prime if it is only divisible by 1 and itself."

positive divisors of 10 : $\{1, 2, 5, 10\}$

positive divisors of 1 : $\{1\}$

2 is prime because its (pos.) divisors are $\underline{1, 2}$

3 is prime " " $\underline{1, 3}$

pattern: every (pos) $n \in \mathbb{N}$ is divisible by 1 and n

open question: how many positive divisors do perfect squares have?

10 has 4 (pos.) divisors

12 has 6 (pos.) divisors

16 has 5 (pos.) divisors

$\{1, 2, 4, 8, 16\}$

Summarize

we prove propositions & theorems

(we will need various definitions to write & understand these proofs)

We will focus on three types of proofs

- Direct Proof
- Contrapositive Proof
- Proof By Contradiction

often good for proving $P \Rightarrow Q$